Department of Justice

Federal Bureau of Investigation

INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS)

SYSTEM REQUIREMENTS DOCUMENT

IAFIS-DOC - 01020 -11.6

FINAL

August 27, 2008

Prepared By:

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306

NGI-518

This Page Intentionally Left Blank

CHANGE HISTORY SECTION

Version/ Revision	Revision Date	Description of Change	QA Approved	Date
—	—	Note: This reflects SPCR 14885—Convert the IAFIS System Requirements Definition from WordPerfect to Word.		
9.0	10/31/2003	SPCR 16364 - Updated the IAFIS System Requirements Definition to reflect changes on IAFIS through summer of 2003. Changed document number from IAFIS-RS-0010 to IAFIS-DOC-01020.		13 Nov 03
9.1	08/22/2005	SPCR 21355 – Update to IAFIS SRD to incorporate changes to support IDENT/IAFIS V1.2 (TPRS)		31-Oct-05
9.2	10/4/2005	SPCR 17727V – Update to reflect changes to support No Value Hops. Also, includes changes to improve requirements traceability. Includes RequisitePro Tags.		13 Dec 05
9.3	2/6/2006	SPCR 23082a – Update to reflect changes to incorporate PI903 III Verify, Auto-Sequence Check, and Search But Don't Add. Update to reflect changes to remove Ten-Print MRD processing. Creation of unique requirement type & numbers with RequisitePro Application – requirements traceability tool.		17 May 06
10.0	12/20/06	SPCR 25455 – This document supersedes the IAFIS System Requirements Definition V9.3. This document adopts a LCMD tailored format and is renamed the System Requirements Document.		07 Mar 07
11.0	5/18/07	SPCR 25968 – This document updated as a result of review process to link IAFIS SRD requirements to the IAFIS System Specification 11.0 requirements within RequisitePro. Original IAFIS SRD Change History section for documenting IAFIS development changes (circa 1991 – 1999) deleted.		19 Jun 07
11.1	06/25/07	SPCR 25612i – This document has been updated to reflect the NGI QuickWin – Quality Check Automation Phase III Option A.		28 Jun 07
11.2	08/14/2007	SPCR 27815a – Contains changes for the EMUF STOT for Build 8.2 (SPCR 26510z)		14 Aug 07

b6
b7C

b6
b7C

11.3	01/17/2008	SPCR 29044b – Contains updates to include existing IAFIS functionality that was documented in the IAFIS System Specification but inadvertently omitted from the IAFIS SRD.		13 Mar 08
11.4	05/9/2008	SPCR 27063i – Contains changes to reflect new requirements to support the receipt and storage of additional biometrics. SPCR 27519w – added TOTs DOCE & NFUE.		23 May 08
11.5	06/18/2008	SPCR 28987c -- NGI QuickWin - Receive and Store 1000ppi Ten-Print transactions. SPCR 30446b – Legacy IAFIS SRD requirements which are currently implemented but not documented in the IAFIS SRD, discovered as a result of NGI Use Case Review. SPCR 30113a – Parent SPCR		09/08/08
11.6	08/27/2008	***Please note this document reflects the requirements baseline maintained in RequisitePro. ALL CHANGES MUST be made in RequisitePro, or changes will not be reflected in later versions of the document.*** ***Contact [redacted] for final versions of the document if any changes or updates are made, including the CM signature box to the right for a final version for the CM document tree.*** ***Each requirement in this document has a requirement number. To view these numbers, go to the MS WORD Tools tab, select Options, then select Hidden Text.***		

b6
b7C

NGI-521

This Page Left Intentionally Blank.

TABLE OF CONTENTS

NGI-525

LIST OF TABLES

This Page Left Intentionally Blank.

1 INTRODUCTION

The Criminal Justice Information Services (CJIS) Division is responsible for the operation and management of three vital criminal justice systems that provide information and data sharing services to the law enforcement community. These systems are the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Instant Criminal Background Check System (NICS).

The IAFIS system provides law enforcement access to fingerprint identification and criminal history services. It also supports real time communications between systems by providing networking interfaces between international, federal, state, tribal, and local agency systems.

The NCIC system maintains a national index to documented theft reports, warrants and other criminal justice information submitted by law enforcement agencies from across the country. It provides law enforcement with access to criminal justice data pertaining to crimes and criminals of national interest.

The NICS system is a national system that provides authorized users with information about persons who may be prohibited by federal or state laws from owning or receiving a firearm.

Together, the systems comprise the CJIS System of Services (SoS), an integrated approach to providing customer information and services that support the detection and reduction of domestic and international terrorist and criminal related activities.

1.1 Purpose of Document

This document, the IAFIS System Requirements Document (SRD), defines the user and functional requirements for the system identified as the Integrated Automated Fingerprint Identification System. These requirements will provide the core IAFIS User Services to the communities served by the FBI.

The requirements contained within this document are intended to be free from design considerations unless there are compelling reasons to constrain the design. Also included are workload and performance requirements for the overall system through the year 2012.

1.2 Background

The CJIS IAFIS, the largest fingerprint identification system in the world, has been instrumental in meeting the fingerprint identification needs of the law enforcement community. Since its inception in July 1999, IAFIS has provided automated ten-print and latent identification and criminal history data for both civil and criminal needs. Continuous improvements and upgrades since then have provided unprecedented increases in system performance, search reliability, throughput and response times.

The tragic events of September 11th 2001 transformed the direction of the FBI and the law enforcement community and highlighted the need for reliable and rapid identification of individuals and the ability to provide and share criminal information across agencies. The adoption of Homeland Security legislation and other national security legislation has spawned the implementation of additional IAFIS services to improve homeland and border security, enhance transportation safety and security, and increase information sharing.

1.3 System Objectives

IAFIS objectives are as follows:

- *Provide accurate and timely services to user agencies*: The FBI provides vital services to support law enforcement agencies and other users nationwide. To accomplish this mission, the FBI's automated systems must supply critical information in a timely manner.
- *Support a paperless environment*: Transactions received from and sent to other organizations, as well as internal FBI transactions, will be electronic to the maximum extent feasible. Since not all external organizations will be fully automated, some paper will be received for many years. Incoming fingerprint cards and documents received in paper form will be converted to digital image form and processed electronically upon receipt.
- *Enable the FBI to process a significant growing workload without increasing staff*: The pressures on the federal budget dictate the use of high performance automation and work re-engineering to cope with increasing workloads.
- *Increase the number of crimes solved by providing enhanced identification and investigative services*: The improvement of both the Ten-Print and latent capabilities of IAFIS will assist law enforcement agencies in solving more crimes.
- *Provide options for IAFIS participation to international, federal, state, tribal and local agencies*: Each option will provide users with access to a different predefined level of IAFIS technical capability, so that each agency can choose the option best suited to its needs. Agencies may continue to mail Ten-Print cards and documents to the FBI for processing, or take full advantage of electronic data transmission and access a greater number of IAFIS capabilities.

1.4 Organization of Document

Following this introduction, section 2 describes the exposed IAFIS user service requirements, section 3 describes the functional requirements, and section 4 contains a description of workload, performance, security, and other non-functional requirements. A bibliography is provided at the end of the document.

2 USER SERVICE REQUIREMENTS

The FBI provides user services to: (1) authorized customers located at law enforcement and criminal justice agencies, (2) others that have an authorized non-criminal justice purposes and (3) FBI staff members who are identified as authorized Service Providers.

There are six core IAFIS services to be provided to these users. The IAFIS user requirements identified below have been listed by these six categories.

2.1 Identification Services

The Identification Service provides a positive or negative identification of an individual based on a one-to-many biometric search.

Ten-Print Fingerprint Identification user requirements are defined as follows.

UR1 IAFIS shall support Ten-Print Fingerprint Identification Search requests.

Ten-Print submissions may be submitted on a hardcopy FBI fingerprint card, or electronically in accordance with the latest Electronic Fingerprint Transmission Standard (EFTS). Fingerprint submissions may be processed by internal Ten-Print or Latent Service Providers who may choose to manually request an identification, non-identification or rejection response in reply to the request.

UR2 IAFIS shall support an Automated Quality Check (AQC) Service for Ten-Print Identification Search Requests.

IAFIS has the capability to make a pass or fail decision through a rule-based Automated Quality Check (AQC) process. Ten-Print Fingerprint submissions which do not pass the automated process are forwarded to an authorized FBI Service Provider for manual review.

UR3 Deleted.

UR4 IAFIS shall provide an appropriate response to a Ten-Print Fingerprint Identification Search request.

A response may include a subject criminal history and/or civil information relevant to the identified subject. IAFIS may provide an electronic or printed response, as requested by the submitter of the request.

UR59 IAFIS shall support Ten-Print Fingerprint Identification Search requests against shared data records.

Ten-Print Fingerprint Identification Search requests against shared data records contained within iDSM may only be submitted by Authorized iDSM Pilot Agencies.

UR5 IAFIS shall provide wanted person information with the Ten-Print Fingerprint Identification Search Response. NGI-531

UR6 IAFIS shall provide flash information with the Ten-Print Fingerprint Identification Search Response.

UR7 IAFIS shall provide sex offender registry information with the Ten-Print Fingerprint Identification Search Response.

UR8 IAFIS shall support a Hot Check Name Search of the NCIC persons' files for Ten-Print Fingerprint Identification Searches.

NCIC will compare the submitted Ten-Print fingerprint search request biographic data to the NCIC Wanted Person File and the terrorists records contained within the NCIC Violent Gang and Terrorist Organization File (VGTOF). NCIC may provide notifications of hits to the NCIC record owner(s).

Latent Fingerprint Identification user requirements are defined as follows.

UR9 IAFIS shall support Latent Fingerprint Identification Search requests.

Latent Fingerprint Identification Search requests will be submitted electronically in accordance with the latest EFTS.

UR10 IAFIS shall provide an appropriate response to a Latent Fingerprint Identification Search request.

Latent Fingerprint identification searches will be processed by internal Latent Service Providers who will provide identification, non-identification or rejection responses in reply to the request.

2.2 Verification Services

The Verification Service provides a confirmation of an identity based on a one-to-one comparison. This service is not currently supported by IAFIS.

2.3 Information Services

The Information Service supports user requests for biographic and/or biometric information for a specific individual.

UR11 IAFIS shall support Criminal History Information Requests containing a unique identifier.

UR12 IAFIS shall support Civil History Information Requests containing a unique identifier.

UR13 Deleted.

III participating states will submit all arrest fingerprints to the FBI for processing. The FBI will maintain a copy of the criminal history for III states, although the state may have a more complete

history. For the purpose of criminal Fingerprint Identification Search responses, the FBI will use its copy of a III state's criminal history.

For external criminal history requests (QR messages) that are done for criminal or national security purposes, the FBI will notify all III states holding portions of the requested record, and they will be responsible for disseminating their criminal histories to the requestor.

UR14 IAFIS shall support the retrieval of NFF Participant State Criminal Records on requests for criminal justice purposes.

NFF participating states will submit only the first arrest for an individual to the FBI. IAFIS will create a "stub" arrest that indicates that all criminal history from the NFF state is maintained at the state level. Subsequent arrests are not submitted to the FBI, but an electronic message is sent to inform the FBI when an individual is re-arrested.

UR15 IAFIS shall support Photo Image Retrieval Requests containing a unique identifier.

UR16 IAFIS shall support Fingerprint Image Requests containing a unique identifier.

UR53 IAFIS shall support Certification File requests.

UR55 IAFIS shall support Other Information Requests.

2.4 Investigation Services

The Investigation Service provides a list of candidates based on a one-to-many biometric and/or biographic search. The result set may include an ordered listing of candidates and corresponding information to facilitate the investigative decision process.

UR17 IAFIS shall support Subject Search Requests based on biographic information.

The search request may be submitted via NCIC, NICS or IAFIS workstations, or MRD.

UR18 IAFIS shall provide a candidate list in response to a Subject Search Request.

The response may contain additional biographical data for each subject or pointers to other systems that may contain additional data.

UR19 IAFIS shall support Latent Image Search Requests of specified repositories.

UR20 IAFIS shall provide a candidate list in response to a Latent Image Search Request.

UR21 IAFIS shall support Latent Feature Search requests of specified repositories.

UR52 IAFIS shall support Unsolved Latent Searches.

UR22 IAFIS shall provide a candidate list in response to a Latent Feature Search request.

UR23 Deleted.

UR39 IAFIS shall support Latent Penetration Searches against IAFIS repositories.

UR40 IAFIS shall support Latent Search Status and Modification Requests.

UR56 IAFIS shall support Latent Repository Statistics Query Requests.

UR41 IAFIS shall support Comparison Fingerprint Image Submissions.

UR42 IAFIS shall support Major Case Image Submissions for Latent Investigations.

UR43 IAFIS shall support Evaluation Latent Fingerprint Submission for investigation.

UR24 IAFIS shall support Fingerprint Image Search Requests against IAFIS fingerprint repositories.

UR25 IAFIS shall provide a candidate list in response to Fingerprint Image Search Requests.

UR26 IAFIS shall support Fingerprint Feature Search requests against IAFIS fingerprint repositories.

UR27 IAFIS shall provide a candidate list in response to a Fingerprint Feature Search request.

UR28 IAFIS shall support Ten-Print Fingerprint Rap Sheet Search Requests of IAFIS repositories.

UR29 IAFIS shall provide a candidate list and corresponding rap sheets in response to a Ten-Print Fingerprint Rap Sheet Search Request.

The search response may contain up to 5 top-scoring candidates in addition to any criminal records associated with those candidates.

UR30 IAFIS shall support Ad Hoc Subject Search requests of subject criminal history repository.

2.5 Notification Services

The Notification Service provides event notification to users. With this service, a data owner will receive an unsolicited notification from the system based on event criteria (triggers).

UR31 IAFIS shall provide notification of record activity on persons who are of special interest.

Special Interest Flags will include Flashes, Wanted Persons, Registered Sexual Offenders, and other persons of special interest.

UR32 IAFIS shall provide notification of file maintenance activities to criminal record owners.

NGI-534

UR54 IAFIS shall provide the owner of an unsolved latent fingerprint with notification of potential fingerprint matches.

UR48 IAFIS shall provide the owner of an unsolved Latent with notifications of deletions due to ULF maximum capacity.

UR49 IAFIS shall support NFF State Criminal Print Ident (CPI) notifications.

UR60 IAFIS shall support Hit Notifications of positive identifications against shared data records.

2.6 Data Management Services

The Data Management Service supports data management by providing authorized users the capability to add, delete, or modify biographic and/or criminal history data.

UR33 IAFIS shall support file maintenance of criminal fingerprint records.

UR44 IAFIS shall support restoration of Subject Criminal History Information.

UR34 IAFIS shall support file maintenance of photos.

UR35 IAFIS shall support file maintenance of latent files.

IAFIS will have capabilities to modify and delete data within the Special Latent Cognizant (SLC) Files and, Unsolved Latent Files (ULF).

UR36 IAFIS shall support file maintenance of contributor information.

UR45 IAFIS shall support the maintenance of Special Stop records.

UR46 IAFIS shall support Death Notice submissions.

UR47 IAFIS shall support Flash Submissions.

UR37 IAFIS shall support file maintenance of Subject Criminal History Records.

IAFIS will support the processing of information related to dispositions, expungements, consolidations, death notices, and want and flash notifications. IAFIS also supports the maintenance of specific biographic and criminal record data.

UR38 IAFIS shall support file maintenance requests for the synchronization of NCIC and IAFIS Wanted Person and Sexual Offender Registry information.

UR50 IAFIS shall support the maintenance of authorized Statutes.

IAFIS will provide the capability to perform statute maintenance for the list of known state statutes used by AQC.

NGI-535

UR57 IAFIS shall support Unsolved Latent Add Confirm submissions.

UR58 IAFIS shall support the maintenance of the Computerized Records Sent File.

UR61 IAFIS shall support the file maintenance of shared data records.

This Page Left Intentionally Blank.

3 FUNCTIONAL REQUIREMENTS

This section identifies the functional requirements derived from the user requirements described in the previous section. Pertinent workload performance, availability, security, and other requirements that must be considered in conjunction with these functional requirements are identified in section 4.

3.1 Identification Services Functional Requirements

The following section contains the functional requirements supporting Identification user services.

3.1.1 Ten-Print Fingerprint Identification Services

The Ten-Print Fingerprint Identification Services will provide the capability to match fingerprint information from criminal and civil Ten-Print submissions to fingerprint information contained within the IAFIS repositories. This service results in an identification decision (i.e., "ident", "non-ident"). If the submission does not meet minimum processing criteria (i.e., quality, etc.), the submission will be returned with a reason for rejection. Ten-Print Fingerprint Identification Search requests submitted by Authorized Pilot Agencies will generate a search of the iDSM independent of the IAFIS search.

3.1.1.1 Ten-Print Fingerprint Identification Inputs

FR1 IAFIS shall accept rolled fingerprint data from an Authorized Contributor as part of a Ten-Print Fingerprint Identification Search request in accordance with the latest EFTS version.

The EFTS Type of Transactions (TOTs) that support the Ten-Print Fingerprint Identification Search include: AMN, CAR, *CARC, CNA, *CNAC, CPDR, CPNU, DEK, DEU, DOCE, EMUF, FANC, FAUF, FIDO, FNDR, *FUFC, LCAR, MAP, *MAPC, MPR, NFAP, *NFDP, *NFFC, NFUE, NFUF, and NNDR. The following TOTs are considered Humanitarian Ten-Print Identification searches: AMN, DEU, and MPR.

* Denotes limited use by Card Scanning Service

FR2 IAFIS shall allow an Authorized FBI Service Provider to submit a Ten-Print Fingerprint Identification Search request.

The internal System Type of Transactions (STOTs) that supports the Ten-Print Fingerprint Identification Search include: IAMN, ICAR, ICNA, IDEK, IDEU, IFANC, IFAUF, FOID, IMAP, IMPR, and INFUF. The following STOTs are considered Humanitarian Ten-Print Identification searches: IAMN, IDEU, and IMPR.

FR663 IAFIS shall accept fingerprint images at 1000ppi from Authorized Contributors as part of a Ten-Print Fingerprint Identification Search request.

NGI-538

FR3 IAFIS shall require a retention status indicator as part of a Ten-Print Fingerprint Identification Search request.

FR4 IAFIS shall accept a photo set as part of a Ten-Print Fingerprint Identification Search request.

FR5 IAFIS shall accept FBI Number (FNU(s)) as part of a Ten-Print Fingerprint Identification Search request.

FR6 IAFIS shall accept a Rap Sheet indicator as part of a Ten-Print Fingerprint Identification Search request.

The Rap Sheet indicator will be used to determine if a Criminal History Rap Sheet should be included as part of a Ten-Print Fingerprint Identification response for a positive identification decision.

FR7 IAFIS shall allow an Authorized FBI Service Provider to scan fingerprint images to initiate a Ten-Print Fingerprint Identification Search request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

FR589 IAFIS shall accept palm print images as part of a Ten-Print Fingerprint Identification Search request from an Authorized Contributor.

FR590 IAFIS shall accept iris data input as part of a Ten-Print Fingerprint Identification Search request from an Authorized Contributor.

3.1.1.2 Ten-Print Fingerprint Identification Processing

FR664 IAFIS shall convert fingerprint images received at 1000ppi to 500ppi for processing as part of a Ten-Print Fingerprint Identification Search request.

FR665 IAFIS shall store all fingerprint images provided in 1000ppi format as part of Ten-Print Fingerprint Search request.

FR592 IAFIS shall generate a Ten-Print Fingeprint Identification Search against the IDENT shared data as a result of a Ten-Print Fingeprint Identification Search request from an Authorized iDSM Pilot Agency.

When an incoming Ten-Print Fingerprint Identification Search request or CPI Notification is from an Authorized iDSM Pilot Agency, IAFIS will not only search against the required repository but will also independently search and compare against the IDENT shared data in iDSM.

FR8 IAFIS shall perform an Automated Quality Check (AQC) of textual data (i.e., reason fingerprinted, arrest data, etc.) contained in a Ten-Print Fingerprint Identification Search request against the AQC business rules.

AQC will verify that the submission textual data meets processing criteria for the TOT. If the AQC fails, the submission will be flagged for manual review or rejection.

IAFIS will provide two options to validate the Reason Fingerprinted (RFP) field for Non-Federal User Fee applicant submissions. Option A will validate the RFP against a list of authorized statutes. Option B will validate the RFP against a list of standardized terms.

FR9 IAFIS shall reject a Ten-Print Fingerprint Identification Search request when textual information is invalid based on AQC business rules.

FR10 IAFIS shall require an Authorized FBI Service Provider to perform Manual Quality Check (QC) on a Ten-Print Fingerprint Identification Search request when AQC business rules determine manual review is necessary.

FR11 IAFIS shall allow an authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search request when it is determined to be invalid as part of Manual QC.

FR12 IAFIS shall perform an Automated Sequence Check (ASC) of the individual fingerprint impressions to the plain fingerprint impressions contained in a Ten-Print Fingerprint Identification Search request to determine if the individual fingerprint impressions are correctly sequenced.

FR13 IAFIS shall reject a Ten-Print Fingerprint Identification Search request as part of ASC when fingerprint data fails to meet processing criteria.

FR14 IAFIS shall automatically extract fingerprint features from the fingerprint images provided in the Ten-Print Fingerprint Identification Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

FR15 IAFIS shall perform an automated image quality check on a Ten-Print Fingerprint Identification Search request based on image quality standards.

FR16 IAFIS shall reject a Ten-Print Fingerprint Identification Search request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

FR17 IAFIS shall require an Authorized FBI Service Provider to perform Manual Fingerprint Sequence Check (FSC) on a Ten-Print Fingerprint Identification Search request when ASC determines that manual review is necessary.

FR18 IAFIS shall allow an Authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search request as part of Manual FSC when fingerprint data fails to meet processing criteria.

FR19 IAFIS shall search fingerprints against the IAFIS repositories, without performing fingerprint file maintenance, when the Ten-Print Fingerprint Identification Search request fails to satisfy fingerprint image quality for retention.

The Search But Don't Add (SBDA) service allows Ten-Print submissions of a defined quality to be used in search of the IAFIS repositories, but not allow the images and features to be added to the IAFIS.

Humanitarian prints will be added despite the SBDA flag being set. If the submitted prints results in a non-identification decision, IAFIS will responds with a quality reject message.

FR593 IAFIS shall search the fingerprint features of the IDENT shared data records as part of a Ten-Print Fingerprint Identification search request submitted by an Authorized iDSM Pilot Agency.

FR520 IAFIS shall reject the Ten-Print Fingerprint Identification Search request when the SBDA indicator is set and the search results in a non-identification decision.

FR20 Deleted.

When an incoming submission references at least one FNU, a fingerprint comparison of each contributor supplied (quoted) FNU is made prior to a technical search and/or name search.

FR21 IAFIS shall search the criminal records in the IAFIS repository for candidates based on biographic data provided as part of a Ten-Print Fingerprint Identification Search request.

FR22 IAFIS shall compare the fingerprint features extracted from the fingerprint images provided in the Ten-Print Fingerprint Identification Search request against the fingerprint features of each candidate provided to the III/Verify Service.

FR23 IAFIS shall perform a III/Verify service for each quoted FNU or Subject Search candidate.

FR24 IAFIS shall determine a "match score" for each candidate resulting from a Ten-Print Identification Search Request.

IAFIS will determine a match score for each quoted FNU, Subject Search candidate or Feature Search candidate.

FR594 IAFIS shall determine a "match score" for each candidate resulting from a feature search of the IDENT shared data contained within iDSM.

FR25 IAFIS shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Ten-Print Identification Search request.

FR26 IAFIS shall automatically determine a "non-Ident" decision for each candidate that has a match score below the minimum threshold for III/Verify as part of a Ten-Print Identification Search Request.

FR27 IAFIS shall search the criminal repository using the fingerprint features extracted from the fingerprint images in the Ten-Print Fingerprint Identification Search request.

The criminal and civil Ten-Print submissions will be searched against the Criminal Ten-Print Fingerprint Features master file. Humanitarian submissions will be searched first against the criminal file. If no identification is made, Humanitarian submissions will then be searched against the civil file.

FR28 IAFIS shall search the civil records in the IAFIS repository for candidates based on biographic data provided as part of a Humanitarian Ten-Print Fingerprint Identification Search request when no identification is made to a criminal record.

A civil Subject Search is only performed for missing person's transactions (i.e., MPR and IMPR Humanitarian TOTs).

FR29 IAFIS shall search the IAFIS civil repository using the fingerprint features extracted from the fingerprint images provided in the Humanitarian Ten-Print Fingerprint Identification Search request when no identification is made to a criminal record.

FR30 IAFIS shall automatically determine an "ident" decision for each candidate that has a match score above the high confidence threshold as part of a Ten-Print Identification Search Request.

Identification decisions may require manual Fingerprint Image Compare (FIC), depending on the match score. If the match score is above the high confidence threshold then no manual FIC is required. If the match score is below the high confidence threshold and above the low confidence threshold then one manual FIC is required. If the match score is below the low confidence threshold then two manual FICs are required.

FR31 IAFIS shall require an Authorized FBI Service Provider to perform an iDSM manual image comparison for each shared data candidate from a Ten-Print Fingerprint Identification Search request that is below the high confidence threshold.

iDSM manual image comparisons performed on candidates resulting from a search of the IDENT shared data records will be performed on IAFIS (ITN) workstations that are independent of normal IAFIS workflow.

FR32 IAFIS shall require a second Authorized FBI Service Provider to perform an iDSM manual image comparison for each shared data candidate from a Ten-Print Fingerprint Identification Search request that is below the low confidence threshold.

FR595 IAFIS shall reject any search request of the IDENT shared data that has been determined "Unable to Process" by three independent manual image comparison service providers.

FR33 IAFIS shall allow an Authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search request as a result of the manual FIC.

FR596 IAFIS shall require an Authorized FBI Service Provider to perform a Post Process Review check on all positive identifications resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

FR34 IAFIS shall retrieve the corresponding subject's criminal history information when requested and a candidate results in an "Ident" decision as part of a Ten-Print Fingerprint Identification Search.

FR35 IAFIS shall retrieve criminal history information from NFF state systems, when appropriate, as part of a Ten-Print Fingerprint Identification Search.

FR531 IAFIS shall combine the IAFIS Ten-Print Fingerprint Identification Search request results with the Criminal History information retrieved from III/NFF State systems, when all III/NFF Criminal History information is available within the response time threshold required to create a combined response.

For the purpose of criminal Fingerprint Identification Search Responses, the FBI will solicit the NFF state for their portion of the criminal history. The response from the NFF state will be appended to the FBI's response and returned to the submitter of the Fingerprint Identification Search. These queries will be sent to states over the NCIC network, the responses sent to IAFIS over Nlets, assembled by IAFIS, and forwarded to the requester to complete a consolidated rap sheet.

FR532 IAFIS shall provide partial Ten-Print Fingerprint Identification Search request results as part of a Ten-Print Fingerprint Identification Search response when III/NFF State systems do not meet the response time threshold required to create a combined response.

FR597 IAFIS shall send an IAQ to LESC, when the daily configured limit is not exceeded, for any positive identification resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

FR598 IAFIS shall accept an IAR from the LESC in accordance with the Nlets Operating Manual.

FR599 IAFIS shall accept an IAR from LESC that contains biographic information for a positive identification resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

The biographic data will consist of DOB, Gender, the IDENT unique identifier (EID), the A-number, FNU, and Subject Name.

FR36 IAFIS shall create a unique subject identifier as a result of a retained Ten-Print Fingerprint Identification Search request that results in a "non-Ident" decision.

FR37 IAFIS shall enroll subject criminal history information for the subject identifier into the appropriate IAFIS repository as a result of a retained Ten-Print Fingerprint Identification Search request that results in a "non-Ident" decision.

FR38 IAFIS shall enroll subject fingerprint information for the subject identifier into the appropriate IAFIS repository based on file maintenance rules as a result of a retained Ten-Print Fingerprint Identification Search request that results in a "non-ident" decision.

FR39 IAFIS shall enroll a photo set for the subject identifier into the appropriate IAFIS repository based on file maintenance rules as a result of a retained Ten-Print Fingerprint Identification Search request containing photos.

FR40 IAFIS shall update subject criminal history information based on file maintenance rules as a result of a Ten-Print Fingerprint Identification Search request with an "Ident" decision.

FR41 Deleted.

FR42 IAFIS shall update fingerprint information based on file maintenance rules as a result of a Ten-Print Fingerprint Identification Search request with an "Ident" decision.

FR43 IAFIS shall create a copy of the Ten-Print Fingerprint Identification Search request for the IAFIS Certification File based on file maintenance rules.

FR44 IAFIS shall perform a Cascaded Fingerprint Search of the ULF as part of the enrollment of fingerprint information provided in a Ten-Print Fingerprint Identification Search request.

FR45 IAFIS shall perform a Cascaded Fingerprint Search of the ULF as part of the update of fingerprint information resulting from a Ten-Print Fingerprint Identification Search request, when appropriate.

FR519 IAFIS shall forward a Hot Check Name Search request to NCIC for all Ten-Print Fingerprint Identification Search requests.

3.1.1.3 Ten-Print Fingerprint Identification Outputs

FR46 IAFIS shall determine the response distribution method (i.e., electronic or hardcopy) for a Ten-Print Fingerprint Identification Search Response.

FR47 IAFIS shall provide an Authorized Contributor with an identification decision when applicable as part of a Ten-Print Fingerprint Identification Search Response.

An identification decision will be either "Ident" or "non-Ident". If the contributor is identified as not being capable of receiving electronic response, a hardcopy response will be generated and sent to the contributor, otherwise an electronic EFTS compliant response will be sent.

FR48 IAFIS shall provide the Subject Criminal History Rap Sheet of an "Ident" candidate in the Ten-Print Fingerprint Identification Search Response when requested.

FR600 IAFIS shall forward an IAR from LESC to the Authorized Pilot Agency as a result of positive identification on a Ten-Print Fingerprint Identification Search request of the IDENT shared data.

FR49 IAFIS shall provide a reject response, as appropriate, for a Ten-Print Fingerprint Identification Search request.

FR50 IAFIS shall provide Authorized Contributors an electronic response to a Ten-Print Fingerprint Identification Search request in accordance with the latest EFTS version.

FR666 IAFIS shall provide all images to Authorized Contributors in 500ppi as part of a Ten-Print Fingerprint Identification Search response.

FR514 IAFIS shall provide the appropriate Ten-Print Fingerprint Identification Search response to an Authorized FBI Service Provider.

FR51 IAFIS shall provide a hardcopy response to a Ten-Print Fingerprint Identification Search request, as appropriate.

FR504 IAFIS shall provide an initial partial response when a Ten-Print Fingerprint Identfcation Search results in a positive identification to a manual record.

NGI 544

3.1.2 Latent Fingerprint Identification Services

The Latent Fingerprint Identification Services will provide the capability to match fingerprint data from Latent Fingerprint Identification Search requests to fingerprint data contained within the IAFIS fingerprint repositories. This service results in an identification decision (i.e., "ident", "non-ident"). If the submission does not meet minimum processing criteria (i.e., quality, etc.), the submission will be returned with a reason for rejection.

3.1.2.1 Latent Fingerprint Identification Inputs

FR52 IAFIS shall accept fingerprint data from an Authorized Contributor as part of Latent Fingerprint Identification Search request in accordance with the latest EFTS version.

The EFTS TOT that supports Latent Fingerprint identification search is LFS.

FR53 IAFIS shall allow an Authorized FBI Service Provider to submit fingerprint data as part of a Latent Fingerprint Identification Search request.

The IAFIS STOT that supports Latent Fingerprint Identification Search is ILFS.

FR54 IAFIS shall allow an authorized FBI Service Provider to scan fingerprint images to initiate a Latent Fingerprint Identification Search request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

FR55 IAFIS shall accept an indicator for enrollment into Unsolved Latent File (ULF) as part of the Latent Fingerprint Identification Search request.

FR56 IAFIS shall accept fingerprint position indicator when a single fingerprint is submitted in a Latent Fingerprint Identification Search request.

An FBI Service Provider can indicate which finger position to search against in the IAFIS repository. If the Latent Fingerprint Identification Search request contains a single fingerprint image, the FBI Service Provider can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

FR57 IAFIS shall require finger position indicator(s) for each fingerprint when multiple fingerprints are submitted as part of a Latent Fingerprint Identification Search request.

FR58 IAFIS shall allow an authorized FBI Service Provider to specify the pattern classification for each fingerprint as part of a Latent Fingerprint Identification Search request.

FR499 IAFIS shall accept a Rap Sheet indicator as part of a Latent Fingerprint Identification Search request.

3.1.2.2 Latent Fingerprint Identification Processing

FR59 IAFIS shall allow an authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Latent Fingerprint Identification Search request.

FR60 Deleted.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

FR61 IAFIS shall allow an authorized FBI Service Provider to initiate automated fingerprint feature extraction to process a Latent Fingerprint Identification Search request.

FR62 IAFIS shall require an authorized FBI Service Provider to extract (i.e., automated or manual) fingerprint features prior to processing a Latent Fingerprint Identification Search request.

FR63 IAFIS shall search the IAFIS repository(s) using the finger position(s) and fingerprint features extracted from the fingerprint images provided in the Latent Fingerprint Identification Search request.

FR64 IAFIS shall search all finger positions for a Latent Fingerprint Identification Search request containing a single fingerprint when no finger position is indicated.

Latent Fingerprint Identification Search requests will be searched first against the criminal file. If no identification is made, the Latent Fingerprint Identification Search request may then be searched against other IAFIS repositories (i.e., civil, Special Latent Cognizant, ULF).

FR660 IAFIS shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Latent Fingerprint Identification Search request.

FR65 IAFIS shall require an Authorized FBI Service Provider to perform a manual Latent Fingerprint Image Compare (LFIC) for each candidate for a Latent Fingerprint Identification Search request.

FR66 IAFIS shall allow an Authorized FBI Service Provider to reject a Latent Fingerprint Identification Search request as a result of the manual FIC.

FR67 IAFIS shall enroll subject information into the ULF, when appropriate, as a result of a Latent Fingerprint Identification Search request.

3.1.2.3 Latent Fingerprint Identification Outputs

FR68 IAFIS shall determine the response distribution method (i.e., electronic or hardcopy) for a Latent Fingerprint Identification Search Response.

FR69 IAFIS shall provide an Authorized Contributor with an identification decision when applicable as part of a Latent Fingerprint Identification Search Response.

NGI-F46

An identification decision will be either "Ident" or "non-Ident".

FR70 IAFIS shall provide the Subject Criminal History Rap Sheet of an "Ident" candidate in the Latent Fingerprint Identification Search Response when requested.

FR71 IAFIS shall provide a reject response, as appropriate, for a Latent Fingerprint Identification Search request.

FR72 IAFIS shall provide a response to a Latent Fingerprint Identification Search request from an Authorized Contributor in accordance with the latest EFTS version.

FR73 IAFIS shall provide a hardcopy response to a Latent Fingerprint Identification Search request, as appropriate.

FR577 IAFIS shall provide the appropriate Latent Fingerprint Identification Search response to an Authorized FBI Service Provider.

3.2 Verification Services Functional Requirements

There are no functional requirements to support IAFIS user verification services.

3.3 Information Services Functional Requirements

The following section contains the functional requirements supporting Information user services.

Image retrieval requests include providing fingerprint images and criminal photos upon request.

3.3.1 Fingerprint Image Retrieval Request

The Fingerprint Image Retrieval Request Services will provide the capability to retrieve fingerprint images contained within the IAFIS repositories. This service results in the return of the requested fingerprint image data for the specified subject.

3.3.1.1 Fingerprint Image Retrieval Request Inputs

FR74 IAFIS shall accept Fingerprint Image Retrieval Requests from Authorized Contributors in accordance with the latest EFTS version.

The EFTS TOT that supports the Fingerprint Image Retrieval Requests is IRQ.

FR75 IAFIS shall allow an Authorized FBI Service Provider to submit a Fingerprint Image Retrieval Request.

The internal STOT that supports the Fingerprint Image Retrieval Requests is IIRQ.

FR76 IAFIS shall allow one or more subject identifiers up to a maximum number as part of a Fingerprint Image Retrieval Request.

3.3.1.2 Fingerprint Image Retrieval Request Processing

FR77 IAFIS shall retrieve the composite fingerprint image for each specified subject as part of the Fingerprint Image Retrieval Request.

FR78 IAFIS shall reject a Fingerprint Image Retrieval Request when the specified subject identifier does not exist.

3.3.1.3 Fingerprint Image Retrieval Request Outputs

FR79 IAFIS shall provide an electronic response to a Fingerprint Image Retrieval Request in accordance with the latest EFTS version.

FR80 IAFIS shall allow an authorized FBI Service Provider to view the images returned from the Fingerprint Image Retrieval Request.

3.3.2 Photo Image Retrieval Request

3.3.2.1 Criminal Photo Image Retrieval Request Inputs

FR81 IAFIS shall accept Criminal Photo Image Retrieval Requests from Authorized Contributors in accordance with the latest EFTS version.

The EFTS TOT that supports the Fingerprint Image Retrieval Requests is CPR.

FR82 IAFIS shall accept a Criminal Photo Image Retrieval Request with a subject identifier and criminal event specific information (i.e., DOA).

3.3.2.2 Criminal Photo Image Retrieval Request Processing

FR83 IAFIS shall retrieve the photo set for the specified criminal event designated in the Criminal Photo Image Retrieval Request.

FR84 IAFIS shall reject a Criminal Photo Image Retrieval request when the specified subject identifier does not exist.

FR85 IAFIS shall reject a Criminal Photo Image Retrieval request when the specified criminal event identifier does not exist.

3.3.2.3 Criminal Photo Image Retrieval Request Outputs

FR86 IAFIS shall provide an electronic response to a Criminal Photo Image Retrieval Request in accordance with the latest EFTS version.

3.3.3 Criminal History Request

3.3.3.1 Criminal History Request Inputs

FR87 IAFIS shall accept Criminal History Request from Authorized Contributors in accordance with the III Operations and Technical Manual.

These requests arrive from the NCIC communications network.

The IAFIS STOT that supports a Criminal History Request is a NCIC Message Key Query Record (QR).

FR667 IAFIS shall accept bulk Criminal History Requests from Authorized Contributors in accordance with the EBTS.

The IAFIS STOT that supports a bulk Criminal History Request is the Electronic Identity History Request (EHIR).

FR88 IAFIS shall allow an Authorized FBI Service Provider to submit Criminal History Request.

The IAFIS STOT that supports Criminal History Request is RRD.

FR89 IAFIS shall accept a FNU as part of a Criminal History Request.

FR542 IAFIS shall accept a CRN from an Authorized FBI Service Provider as part of a Criminal History Request.

FR90 IAFIS shall accept a SID as part of a Criminal History Request.

FR578 IAFIS shall provide the capability for the authorized FBI Service Provider to request a Record Set Report as part of the Criminal History Request.

FR661 IAFIS shall provide the capability for an Authorized FBI Service Provider to request a Receiving Agency Notification Report (RANR) as part of the Criminal History Request.

3.3.3.2 Criminal History Request Processing

FR91 IAFIS shall retrieve the Criminal History information for the specified subject as part of the Criminal History Request.

FR543 IAFIS shall send Criminal History Requests to the III particating states that hold portions of the requested record as part of the Criminal History Request from an Authorized Contributor.

The III particating states will not respond to IAFIS, but will send their Criminal History Information directly to the Authorized Contributor that orginated the Criminal History Request.

FR92 IAFIS shall send a NFF Criminal History Information request to NFF state system when appropriate as a result of a Criminal History Request.

These queries will be sent to states over the NCIC network, the responses sent to IAFIS over Nlets.

FR93 IAFIS shall send a NFF Criminal History Information Request to NFF state system in accordance with the III/NFF Operations and Technical Manual.

FR94 IAFIS shall receive a NFF Criminal History Information response in accordance with the Nlets Operating Manual.

FR95 IAFIS shall combine NFF Criminal History Information Response(s) and IAFIS Criminal History Information into a single Criminal History Response.

FR96 IAFIS shall reject a Criminal History Request when the specified subject identifier does not exist.

3.3.3.3 Criminal History Request Outputs

FR97 IAFIS shall determine the response distribution method (i.e., electronic or hardcopy) for a Criminal History Request response.

FR530 IAFIS shall provide a response to a Criminal History request received via NCIC in accordance with the latest III/NFF Operational.and Technical Manual.

FR98 IAFIS shall provide the Subject Criminal History Rap Sheet for the specified subject in a Criminal History Request response.

FR99 Deleted.

FR100 IAFIS shall provide a hardcopy response to a Criminal History Request, as appropriate.

FR101 IAFIS shall allow an authorized FBI Service Provider to view the Criminal History Request response.

FR516 IAFIS shall allow an authorized FBI Service Provider to print the Criminal History Request response.

FR579 IAFIS shall provide the Record Set Report when requested for the specified subject as part of the Criminal History Request response.

FR662 IAFIS shall provide the RANR when requested for the specified Identity as part of the Criminal History Request response.

3.3.4 Certification File Request

3.3.4.1 Certification File Request Inputs

FR102 IAFIS shall allow an Authorized FBI Service Provider to submit Certification File Request.

FR103 IAFIS shall accept a Subject Identifier as part of a Certification File Request.

FR104 IAFIS shall accept a unique transaction identifier as part of a Certification File Request.

The unique identifier will allow IAFIS to retrieve the specific transaction certification file.

3.3.4.2 Certification File Request Processing

FR105 IAFIS shall retrieve the Criminal History Information for the specified subject and unique event as part of the Certification File Request.

FR106 IAFIS shall reject the Certification File Request when the Subject Identifier or transaction identifier is invalid.

3.3.4.3 Certification File Request Outputs

FR107 IAFIS shall allow an authorized FBI Service Provider to view the Certification File Request response.

FR108 IAFIS shall allow an authorized FBI Service Provider to print the Certification File Request response.

3.3.5 Other Information Requests

Other information requests processed by IAFIS include the Record Availability Inquiry, Record Status Inquiry, and the Administrative Inquiry. The Record Availability Inquiry (ZR) is used to determine, by providing a FBI or SID number, if a subject record is on file in the III. The Record Status Inquiry (ZRS) is used when a III participant wants to verify the status, single- or multi-state, of a subject record. The Administrative Inquiry (ZI) is used by III participants when there is a need to determine: the presence of a SID or FBI pointer and the date established; single-, multi-state or wanted status; or dates of establishment and/or last update

3.3.5.1 Other Information Requests Inputs

FR544 IAFIS shall accept Record Availability Inquiries Requests in accordance with the III/NFF Operations and Technical Manual.

The IAFIS STOT that supports a Record Availability Inquiry is ZR.

FR545 IAFIS shall accept an FNU as part of a Record Availability Inquiry Request.

FR546 IAFIS shall accept a SID as part of a Record Availability Inquiry Request.

FR547 IAFIS shall accept Record Status Inquiry Requests in accordance with the III/NFF Operations and Technical Manual.

The IAFIS STOT that supports a Record Status Inquiry is ZRS.

FR548 IAFIS shall accept an FNU as part of a Record Status Inquiry Request.

FR549 IAFIS shall accept a SID as part of a Record Status Inquiry Request.

FR550 IAFIS shall accept Administrative Inquiries in accordance with the III/NFF Operations and Technical Manual.

The IAFIS STOT that supports an Administrative Inquiry is ZI.

FR551 IAFIS shall accept an FNU as part of an Administrative Inquiry Request.

FR552 IAFIS shall accept a SID as part of an Administrative Inquiry Request.

These requests arrive from the NCIC communications network.

3.3.5.2 Other Information Requests Processing

FR553 IAFIS shall determine if a subject exists in the Subject Criminal History File using the FBI number or SID as part of a Record Availability Inquiry Request.

FR554 IAFIS shall determine the status of the subject in the Subject Criminal History File using the FBI number or SID as part of a Record Status Inquiry Request.

FR555 IAFIS shall retrieve biographic data and III pointer information as part of an Administrative Inquiry Request.

3.3.5.3 Other Information Requests Outputs

FR556 IAFIS shall provide a response to a Record Availability Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

FR557 IAFIS shall provide a response to a Record Status Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

FR558 IAFIS shall provide a response to an Administrative Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

3.4 Investigation Services Functional Requirements

The following section contains the functional requirements supporting Investigation user services.

3.4.1 Subject Search Request

The Subject Search service includes determination of criminal history or felony history based upon search using biographic descriptors such as name, date of birth, sex, and race. A Subject Search Request contains biographic descriptors from which IAFIS generates a list of possible candidate matches.

3.4.1.1 Subject Search Request Inputs

FR109 IAFIS shall accept Subject Search Requests in accordance with the III/NFF Operations and Technical Manual.

These requests arrive from the NCIC communications network.

NGI-552

The IAFIS STOT that supports a Subject Search Request is a NCIC Message Key Query History (QH).

FR110 IAFIS shall accept a Subject Search Request via Machine Readable Data in accordance with the MRD Subject Search Manual.

The IAFIS STOT that supports Subject Search Request via MRD is SSRM.

FR111 IAFIS shall allow an Authorized FBI Service Provider to submit a Subject Search Request.

The IAFIS STOTs that support Subject Search Requests are SPSS and FASS. The SPSS may be initiated by either an IAFIS or a NICS FBI Service Provider.

FR112 IAFIS shall allow an Authorized FBI Service Provider to designate a repository as part of a Subject Search Request.

FR113 IAFIS shall accept biographic data as part of a Subject Search Request.

IAFIS will allow Subject Identifiers (i.e., FNU, CRN, SID) as biographic descriptor data in addition to name, DOB, sex, race, etc. for a Subject Search Request.

FBI numbers and SIDs are unique. Therefore, if either number is used as a descriptor, the search of the file is bypassed and the single candidate record is retrieved from the file. If no record in the file matches, a "no record" message is provided.

3.4.1.2 Subject Search Request Processing

FR114 IAFIS shall search the repository designated as part of the Subject Search Request.

FR115 IAFIS shall search the Subject Criminal History repository by default when no repository is designated in the Subject Search Request.

FR116 IAFIS shall perform a search using the biographic data contained in Subject Search Request.

FR117 IAFIS shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as the result of the Subject Search Request.

3.4.1.3 Subject Search Request Outputs

FR118 IAFIS shall determine the response distribution method (i.e., electronic or hardcopy) for a Subject Search Request response.

FR119 IAFIS shall provide an electronic response to a Subject Search Request in accordance with the III/NFF Operations and Technical Manual.

FR120 IAFIS shall provide a candidate list in response to a MRD Subject Search Request in accordance with the MRD Subject Search Manual.

FR121 IAFIS shall provide a hardcopy of candidate criminal history Rap Sheet for each candidate in response to an MRD Subject Search Request.

NGI-553

FR122 IAFIS shall allow an authorized FBI Service Provider to view the candidate list returned from the Subject Search Request.

FR123 IAFIS shall allow an authorized FBI Service Provider to view the record set returned as the single candidate from the Subject Search Request.

FR124 IAFIS shall allow an authorized FBI Service Provider to print the candidate list returned from the Subject Search Request.

FR125 IAFIS shall allow an authorized FBI Service Provider to print the record set returned as the single candidate from the Subject Search Request.

3.4.2 Ad Hoc Subject Search

The Ad Hoc Subject Search service will support service provider queries of the Subject Criminal History File or the Civil Subject Index Master File. This service allows an FBI Service Provider to search on any biographic or criminal history data elements within the IAFIS Subject Criminal History File or the Civil Subject Index Master File. The response for the search is a candidate list containing zero or more candidates.

3.4.2.1 Ad Hoc Subject Search Inputs

FR126 IAFIS shall allow an Authorized FBI Service Provider to submit an Ad Hoc Subject Search request.

The IAFIS STOT that supports Ad Hoc Subject Search requests is AHSS.

FR127 IAFIS shall allow an Authorized FBI Service Provider to designate an IAFIS subject history file as part of the Ad Hoc Subject Search request.

The FBI Service Provider may direct the Ad Hoc Subject Search against either the Subject Criminal History File or the Civil Subject Index Master File.

FR128 IAFIS shall accept biographic data as part of an Ad Hoc Subject Search request.

IAFIS will allow Subject Identifiers (i.e., FNU, CRN, SID) as biographic descriptor data in addition to name, DOB, sex, race, etc. for a Subject Search Request.

FR129 IAFIS shall accept criminal history data as part of an Ad Hoc Subject Search request.

3.4.2.2 Ad Hoc Subject Search Processing

FR130 IAFIS shall search the repository designated as part of the Ad Hoc Subject Search request.

FR131 IAFIS shall search the Subject Criminal History repository by default when no repository is designated in the Ad Hoc Subject Search request.

FR132 IAFIS shall perform a search using the biographic data contained in the Ad Hoc Subject Search request.

FR133 IAFIS shall perform a search using the criminal history data contained in the Ad Hoc Subject Search request.

3.4.2.3 Ad Hoc Subject Search Outputs

FR134 IAFIS shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as a response to the Ad Hoc Subject Search request.

FR135 IAFIS shall allow an Authorized FBI Service Provider to view the candidate list returned from the Ad Hoc Subject Search request.

FR136 IAFIS shall allow an Authorized FBI Service Provider to print the candidate list returned from the Ad Hoc Subject Search request.

FR137 IAFIS shall allow an authorized FBI Service Provider to copy the Ad Hoc Subject Search resulting candidate(s) to a SLC File.

Only a limited number of Authorized Service Providers will be provided the capability to copy Ad Hoc Subject Search candidate(s) to a SLC.

3.4.3 Ten-Print Fingerprint Image Search

An Authorized Contributor will be able to submit a Ten-Print Fingerprint Image Search request with fingerprint images, fingerprint classification information, and biographic descriptors. The response consists of a candidate list and the fingerprint images of the highest ranked candidate. Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests.

3.4.3.1 Ten-Print Fingerprint Image Search Inputs

FR138 IAFIS shall accept Ten-Print Fingerprint Image Search requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Ten-Print Fingerprint Image Search request is TPIS.

FR139 IAFIS shall require fingerprint image data as part of a Ten-Print Fingerprint Image Search request.

FR140 IAFIS shall accept biographic descriptor data as part of a Ten-Print Fingerprint Image Search request.

FR141 IAFIS shall accept fingerprint classification information as part of a Ten-Print Fingerprint Image Search request.

3.4.3.2 Ten-Print Fingerprint Image Search Processing

FR142 IAFIS shall perform an automated image quality check on a Ten-Print Fingerprint Image Search request based on image quality standards.

FR143 IAFIS shall reject a Ten-Print Fingerprint Image Search request when the fingerprint images fail to satisfy minimum image quality standards.

FR144 IAFIS shall automatically extract fingerprint features from the fingerprint images provided in the Ten-Print Fingerprint Image Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

FR145 IAFIS shall search the IAFIS criminal fingerprint repository using the fingerprint classification data, biographic data, and extracted fingerprint features from the Ten-Print Fingerprint Image Search requests.

FR146 IAFIS shall retrieve the composite fingerprint images for the highest ranking candidate as a result of Ten-Print Fingerprint Image Search request.

3.4.3.3 Ten-Print Fingerprint Image Search Outputs

FR147 IAFIS shall provide a response to a Ten-Print Fingerprint Image Search request in accordance with the latest EFTS version.

FR148 IAFIS shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as a result of the Ten-Print Fingerprint Image Search request.

3.4.4 Ten-Print Fingerprint Feature Search

The Ten-Print Fingerprint Feature Search requests will allow an Authorized Contributor to search using fingerprint features, pattern classification and biographic descriptors. The response consists of a candidate list and the fingerprint images of the highest ranked candidate. Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests.

3.4.4.1 Ten-Print Fingerprint Feature Search Inputs

FR149 IAFIS shall accept Ten-Print Fingerprint Feature Search requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Ten-Print Fingerprint Feature Search request is TPFS.

FR150 IAFIS shall require fingerprint feature data as part of a Ten-Print Fingerprint Feature Search request.

FR151 IAFIS shall accept fingerprint classification information as part of a Ten-Print Fingerprint Feature Search request.

FR152 IAFIS shall accept biographic descriptor data as part of a Ten-Print Fingerprint Feature Search Request.

3.4.4.2 Ten-Print Fingerprint Feature Search Processing

FR153 IAFIS shall search the IAFIS criminal fingerprint repository using the fingerprint feature, fingerprint classification, and biographic data contained within the Ten-Print Fingerprint Feature Search request.

FR154 IAFIS shall retrieve the composite fingerprint images for the highest ranking candidate as a result of Ten-Print Fingerprint Feature Search request.

3.4.4.3 Ten-Print Fingerprint Feature Search Outputs

FR155 IAFIS shall provide a response to a Ten-Print Fingerprint Feature Search request in accordance with the latest EFTS version.

FR156 IAFIS shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as a result of the Ten-Print Fingerprint Feature Search request.

3.4.5 Ten-Print Fingerprint Rap Sheet Search

An Authorized Contributor will submit a Ten-Print Fingerprint Rap Sheet Search request with fingerprint images, fingerprint classification information, and biographic descriptors. The response will consist of a candidate list and the corresponding rap sheets.

3.4.5.1 Ten-Print Fingerprint Rap Sheet Search Inputs

FR157 IAFIS shall accept Ten-Print Search Rap Sheet Search Request from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Ten-Print Fingerprint Search Rap Sheet Search request is TPRS.

FR158 IAFIS shall require fingerprint image data as part of a Ten-Print Fingerprint Rap Sheet Search Request.

FR159 IAFIS shall accept biographic descriptor data as part of a Ten-Print Fingerprint Rap Sheet Search Request.

FR160 IAFIS shall accept fingerprint classification information as part of a Ten-Print Fingerprint Rap Sheet Search Request.

3.4.5.2 Ten-Print Fingerprint Rap Sheet Search Processing

FR161 IAFIS shall perform an automated image quality check on a Ten-Print Fingerprint Rap Sheet Search request based on image quality standards.

FR162 IAFIS shall reject a Ten-Print Fingerprint Rap Sheet Search request when the fingerprint images fail to satisfy minimum image quality standards.

FR163 IAFIS shall automatically extract fingerprint features from the fingerprint images provided in the Ten-Print Fingerprint Rap Sheet Search Request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

FR164 IAFIS shall search the criminal fingerprint repository using the fingerprint classification data and extracted fingerprint features from the Ten-Print Fingerprint Rap Sheet Search Request.

FR165 IAFIS shall retrieve the subject criminal history identifier and rap sheet for the highest ranked candidate(s) up to the maximum number as a result of Ten-Print Fingerprint Rap Sheet Search Request.

3.4.5.3 Ten-Print Fingerprint Rap Sheet Search Outputs

FR166 IAFIS shall provide a response to a Ten-Print Fingerprint Rap Sheet Search request in accordance with the latest EFTS version

The search response may contain up to 5 top-scoring candidates in addition to any subject criminal history records associated with those candidates.

FR167 IAFIS shall provide the Subject Criminal History Rap Sheet for all candidates in the Ten-Print Fingerprint Rap Sheet Search Response.

3.4.6 Latent Penetration Query

The Latent Penetration Query request allows the user to receive an estimated percentage of the IAFIS criminal repository that will be accessed by a Latent Fingerprint Image Search request or a Latent Fingerprint Feature Search request. The query contains the search parameters that will be defined in the search but no images or features. This will allow setting the search parameters to ensure that the maximum penetration allowed is not exceeded.

3.4.6.1 Latent Penetration Query Inputs

FR168 IAFIS shall accept Latent Penetration Query requests from Authorized Contributors in accordance with the latest EFTS version.

The EFTS TOT that supports the Latent Penetration Query requests is LPNQ.

FR169 IAFIS shall allow an Authorized FBI Service Provider to submit a Latent Penetration Query request.

The IAFIS STOT that supports Latent Penetration Query Requests is ILPNQ.

3.4.6.2 Latent Penetration Query Processing

FR170 IAFIS shall calculate the estimated percentage of the IAFIS criminal repository that would be searched using the latent search parameters provided in the Latent Penetration Query request.

3.4.6.3 Latent Penetration Query Outputs

FR171 IAFIS shall provide an electronic response to a Latent Penetration Query request in accordance with the latest EFTS version.

FR172 IAFIS shall allow an authorized FBI Service Provider to view the results of the Latent Penetration Query request. NGI-558

3.4.7 Latent Fingerprint Image Search

An Authorized Contributor will be able to submit a Latent Fingerprint Image Search request with a fingerprint image(s), fingerprint classification information, and biographic descriptors. The response consists of a candidate list of FNUs and fingerprint images.

3.4.7.1 Latent Fingerprint Image Search Inputs

FR173 IAFIS shall accept Latent Fingerprint Image Search requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Latent Fingerprint Image Search request is LFIS.

FR174 IAFIS shall require one or more fingerprint images as part of a Latent Fingerprint Image Search request.

FR175 IAFIS shall allow one or more finger position indicators when a single fingerprint is submitted in a Latent Fingerprint Image Search request.

An Authorized Contributor can indicate which finger position to search against in the IAFIS repository. If the Latent Fingerprint Image Search request contains a single fingerprint image, the contributor can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

FR176 IAFIS shall search all finger positions for a Latent Fingerprint Image Search request containing a single fingerprint and no finger position indicator.

FR177 IAFIS shall require a finger position indicator for each fingerprint image when multiple fingerprint images are contained in the Latent Fingerprint Image Search request.

FR178 IAFIS shall accept biographic descriptor data as part of a Latent Fingerprint Image Search request.

FR179 IAFIS shall accept fingerprint classification information as part of a Latent Fingerprint Image Search request.

FR180 IAFIS shall accept an indicator for enrollment in the ULF as part of the Latent Fingerprint Image Search request.

3.4.7.2 Latent Fingerprint Image Search Processing

FR181 IAFIS shall perform an automated image quality check on a Latent Fingerprint Image Search request based on image quality standards.

FR182 IAFIS shall reject a Latent Fingerprint Image Search request when the fingerprint images fail to satisfy minimum image quality standards.

FR183 IAFIS shall automatically extract fingerprint features from the fingerprint image(s) provided in the Latent Fingerprint Image Search request.

NGI-559

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae,

core/delta locations, and quality metrics.

FR184 IAFIS shall search the criminal fingerprint repository as part of a Latent Fingerprint Image Search request.

FR185 IAFIS shall perform the Latent Fingerprint Image search using the finger position, fingerprint classification data, biographic data, and extracted fingerprint features from the Latent Fingerprint Image Search request.

IAFIS will return 20 candidate FNUs as the result of a Latent Fingerprint Image Search request.

FR186 IAFIS shall retrieve the composite fingerprint images for each candidate as a result of Latent Fingerprint Image Search request.

FR187 IAFIS shall enroll subject information into the ULF, when indicated, as a result of a Latent Fingerprint Image Search request.

3.4.7.3 Latent Fingerprint Image Search Outputs

FR188 IAFIS shall provide a response to a Latent Fingerprint Image Search request in accordance with the latest EFTS version.

FR189 IAFIS shall provide a ranked candidate list of a default number of FNUs as a result of the Latent Fingerprint Image Search request.

3.4.8 Latent Fingerprint Feature Search

The Latent Fingerprint Feature Search requests will allow an Authorized Contributor to search using fingerprint features, pattern classification and biographic descriptors. The response consists of a candidate list of FNUs and fingerprint images.

3.4.8.1 Latent Fingerprint Feature Search Inputs

FR190 IAFIS shall accept Latent Fingerprint Feature Search requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Latent Fingerprint Feature Search request is LFFS.

FR191 IAFIS shall require fingerprint feature data from one or more fingerprints as part of a Latent Fingerprint Feature Search Request.

FR192 IAFIS shall accept fingerprint classification information as part of a Latent Fingerprint Feature Search Request.

FR193 IAFIS shall allow one or more finger position indicators when a single fingerprint is submitted in a Latent Fingerprint Feature Search Request.

An Authorized Contributor can indicate which finger position to search against in the IAFIS repository. If the Latent Fingerprint Feature Search request contains a single fingerprint image, the contributor can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

FR194 IAFIS shall require a finger position indicator for each fingerprint image when multiple fingerprint images are contained in the Latent Fingerprint Feature Search request.

FR195 IAFIS shall accept biographic descriptor data as part of a Latent Fingerprint Feature Search request.

FR196 IAFIS shall accept an indicator for enrollment in the ULF as part of the Latent Fingerprint Feature Search request.

3.4.8.2 Latent Fingerprint Feature Search Processing

FR197 IAFIS shall search the criminal fingerprint repository as part of a Latent Fingerprint Feature Search request.

FR198 IAFIS shall perform the Latent Fingerprint Feature search using the finger position, fingerprint classification data, biographic data, and extracted fingerprint features from the Latent Fingerprint Feature Search request.

IAFIS will return 20 candidate FNUs as the result of a Latent Fingerprint Feature Search request.

FR199 IAFIS shall retrieve the composite fingerprint images for each candidate as a result of Latent Fingerprint Feature Search request.

FR200 IAFIS shall enroll subject information into the ULF, when indicated, as a result of a Latent Fingerprint Feature Search request.

FR500 Deleted.

3.4.8.3 Latent Fingerprint Feature Search Outputs

FR201 IAFIS shall provide a response to a Latent Fingerprint Feature Search request in accordance with the latest EFTS version.

FR202 IAFIS shall provide a ranked candidate list of a default number of FNUs as a result of the Latent Fingerprint Feature Search request.

3.4.9 Unsolved Latent Search

Ten-Print Fingerprint searches and latent searches against the ULF.

3.4.9.1 Unsolved Latent Search Inputs

FR203 Deleted.

The EFTS TOTs that support the Unsolved Latent Search requests are ULS and ULTS.

FR204 IAFIS shall allow an Authorized FBI Service Provider to submit fingerprint data as part of an Unsolved Latent Search request.

The IAFIS STOTs that support Unsolved Latent Search requests are IULS and IULTS.

NGI-561

FR205 IAFIS shall allow an authorized FBI Service Provider to scan fingerprint data to initiate an Unsolved Latent Search request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

FR206 IAFIS shall allow one or more fingerprint images as part of an Unsolved Latent Search request.

IAFIS will allow Ten-Print fingerprint data or latent data to be searched against the ULF.

FR207 IAFIS shall allow one or more finger position indicators when a single fingerprint is submitted in an Unsolved Latent Search request.

An Authorized Contributor or FBI Service Provider can indicate which finger position to search against in the IAFIS repository. If the Unsolved Latent Search request contains a single fingerprint image, the Contributor or Service Provider can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

FR208 IAFIS shall require a finger position indicator for each fingerprint image when multiple fingerprint images are contained in the Unsolved Latent Search request.

FR209 IAFIS shall accept fingerprint classification information as part of an Unsolved Latent Search request.

3.4.9.2 Unsolved Latent Search Processing

FR210 IAFIS shall allow an authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Unsolved Latent Search request.

FR211 IAFIS shall provide an automated method to extract fingerprint features from the fingerprint images provided in the Unsolved Latent Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

FR212 IAFIS shall search the ULF using the finger position, fingerprint features, and fingerprint classification contained within the Unsolved Latent Search request.

FR213 IAFIS shall search all finger positions for an Unsolved Latent Search request containing a single fingerprint and no finger position indicator.

3.4.9.3 Unsolved Latent Search Request Outputs

FR214 Deleted.

FR215 IAFIS shall provide a ranked candidate list of a default number of FNUs as a part of the Unsolved Latent Search request response.

FR216 IAFIS shall allow an authorized FBI Service Provider to view the candidate list returned from the Unsolved Latent Search request.

3.4.10 Latent Search Status and Modification Request

Latent Search Status and Modification Request provides an Authorized Contributor or Authorized FBI Service Provider the ability to check the status of a latent search request, adjust priorities, adjust search order, or cancel a previously submitted latent search that are queued in IAFIS. If the Latent Search is already in process, this request will be rejected.

3.4.10.1 Latent Search Status and Modification Request Inputs

FR217 IAFIS shall accept Latent Search Status and Modification Request from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Latent Search Status and Modification Request is LSMQ.

FR218 IAFIS shall allow an Authorized FBI Service Provider to submit a Latent Search Status and Modification Request.

The IAFIS STOT that supports Latent Search Status and Modification Request is ILSMQ.

FR219 IAFIS shall allow Query Depth Detail (QDD) (i.e., ORI, state indicator, EID, case number and extension) as part of the Latent Search Status and Modification Request.

FR220 IAFIS shall require SCNA(s) to modify the status of previously submitted Latent Search(es) as part of the Latent Search Status and Modification Request.

3.4.10.2 Latent Search Status and Modification Request Processing

FR580 IAFIS shall retrieve the AFIS segment process control number (SCNA) of the referenced Latent Search(es) and the estimated time(s) to complete the search(es) when status request indicated as part of the Latent Search Status and Modification Request.

FR221 IAFIS shall modify the priority of the specified Latent Search(es) when indicated as part of the Latent Search Status and Modification Request.

FR222 IAFIS shall change processing order of the specified Latent Search(es) when indicated as part of the Latent Search Status and Modification Request.

FR223 IAFIS shall cancel the specified SCNA(s) Latent Search(es) when indicated as part of the Latent Search Status and Modification Request.

FR224 IAFIS shall reject the Latent Search Status and Modification Request when specified Latent Search(es) are not found in the Latent Search queue.

3.4.10.3 Latent Search Status and Modification Request Outputs

FR225 IAFIS shall provide the appropriate response to the Latent Search Status and Modification Request in accordance with the latest EFTS version.

FR226 IAFIS shall allow an FBI Service Provider to view the Latent Search Status and Modification Request results.

3.4.11 Latent Repository Statistics Query

The Latent Repository Statistics Query request allows the user to receive a statistical representation, based on descriptive data, of a latent repository and is used in updating a user's statistical representation to be used in a penetration query.

3.4.11.1 Latent Repository Statistics Query Inputs

FR559 IAFIS shall accept Repository Statistics Query requests from Authorized Contributors in accordance with the latest EFTS version.

The EFTS TOT that supports the Repository Statistics Query requests is LRSQ.

3.4.11.2 Latent Repository Statistics Query Processing

FR560 IAFIS shall calculate a statistical representation of the descriptors in the Latent Cognizant File using the descriptive data provided in the Latent Repository Statistics Query request.

3.4.11.3 Latent Repository Statistics Query Outputs

FR561 IAFIS shall provide a response to a Latent Repository Statistics Query request in accordance with the latest EFTS version.

3.4.12 Comparison Fingerprint Image(s) Submission (CFS)

The Comparison Fingerprint Image(s) Submission (CFS) supports the comparison of provided Ten-Print fingerprint images or other known prints against the provided latent impressions associated with a case. The CFS is intended solely for FBI use (i.e., field offices, FBI investigators). The provided fingerprints may consist of the following:

1. Suspect known prints
2. Victim known prints
3. Known prints from individuals being compared for purposes of elimination
4. Other individuals involved in the case

The CFS may include all the fingerprints normally enclosed in a Ten-Print submittal plus optional additional prints (e.g., palm prints), if applicable. The submitted fingerprints and latent prints will be analyzed and compared by an Authorized FBI Service Provider (Latent Examiner). Fingerprints for several individuals must be sent as individual submissions. NGI-564 electronic response is returned for this

submission. The contributor will be manually (i.e., telephonically, email, mail, fax) notified of comparison results.

3.4.12.1 Comparison Fingerprint Image Submission Inputs

FR227 IAFIS shall accept Comparison Fingerprint Image Submission from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Comparison Fingerprint Image Submission is CFS.

FR228 IAFIS shall require fingerprint image and latent image data as part of a Comparison Fingerprint Image Submission.

FR229 IAFIS shall accept palm print image data as part of a Comparison Fingerprint Image Submission.

3.4.12.2 Comparison Fingerprint Image Submission Processing

FR230 IAFIS shall require an Authorized FBI Service Provider to perform a manual Latent Fingerprint Image Compare for each set of subject prints provided against latent prints provided as part of a Comparison Fingerprint Image Submission.

3.4.12.3 Comparison Fingerprint Image Submission Outputs

FR517 IAFIS shall allow an Authorized FBI Service Provider to view the response to a Comparison Fingerprint Image Submission.

FR518 IAFIS shall allow an Authorized FBI Service Provider to print the response to a Comparison Fingerprint Image Submission.

IAFIS does not generate a response for Comparison Fingerprint Image Submissions, other than a communication protocol level acknowledgement. The Authorized FBI Service Provider (Latent Examiner) who is assigned to the case and performed the Latent Fingerprint Image Compare will be responsible for producing a report, and subsequently contact the submitting Authorized Contributor.

3.4.13 Major Case Image(s) Submission (MCS) Request

The Major Case Image Submission (MCS) provides for the submission of Ten-Print fingerprints plus additional images of the extreme tips, sides, and lower joints of the fingers, and surface and extreme sides of palms for possible use in comparisons for a case. The MCS is intended solely for FBI use in conjunction with a Latent Print Unit investigation. The submitted prints will be added to the Major Case Image File. In addition, the Ten-Prints may be searched against the criminal fingerprint databases, and providing that all required data is submitted, it may be used to establish a new record in the criminal subject databases or to update existing records on the subject. No electronic response is returned for this request.

3.4.13.1 Major Case Image Submission Inputs

FR231 IAFIS shall accept Major Case Image Submission from Authorized Contributors in accordance with the latest EFTS version. NGI-565

The EFTS TOT that supports the Major Case Image Submission requests is MCS.

The Major Case Image Submission request is limited to FBI staff (e.g., field offices, etc).

FR232 IAFIS shall accept fingerprint image(s) data as part of a Major Case Image Submission.

FR233 IAFIS shall accept supplementary print image(s) data as part of a Major Case Image Submission.

FR234 IAFIS shall accept a Latent Case Number as part of a Major Case Image Submission.

3.4.13.2 Major Case Image Submission Processing

FR235 IAFIS shall enroll the fingerprint image(s) and supplementary print image(s) and Latent Case Number reference contained in a Major Case Image Submission into the Major Case Print File.

3.4.13.3 Major Case Image Submission Outputs

IAFIS does not generate a response for Major Case Image Submission, other than a communication protocol level acknowledgement.

3.4.14 Evaluation Latent Fingerprint Submission Request

The Evaluation Latent Fingerprint Submission Request (ELR) provides the capability for FBI field office personnel to have FBI Latent Fingerprint Section (LFPS) consult on cases. The ELR contains set of latent fingerprints. The ELR is processed similar to a Latent Identification Search Request. The FBI LFPS will contact the Authorized Contributor (FBI field office) with results which may include the establishment of a latent case, a request for additional information, or an evaluation of the case feasibility and recommendations for further actions.

3.4.14.1 Evaluation Latent Fingerprint Submission Request Inputs

FR236 IAFIS shall accept Evaluate Latent Fingerprint Submission Search Requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Evaluate Latent Fingerprint Submission Search Request is ELR.

3.4.14.2 Evaluation Latent Fingerprint Submission Request Processing

FR237 IAFIS shall allow an authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Request.

FR238 IAFIS shall provide an automated method to extract fingerprint features from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI-566

FR239 IAFIS shall allow Authorized FBI Service Provider to search the IAFIS repository(s) using the finger position(s) and fingerprint features extracted from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Request.

Evaluation Latent Fingerprint Submission Request will be searched first against the criminal file. If no identification is made, the Evaluation Latent Fingerprint Submission Request may then be searched against other IAFIS repositories (i.e., civil, Special Latent Cognizant, ULF).

FR240 IAFIS shall allow an Authorized FBI Service Provider to perform a manual Latent Fingerprint Image Compare (LFIC) for each candidate for an Evaluation Latent Fingerprint Submission Request.

FR241 IAFIS shall allow Authorized FBI Service Provider to enroll subject information into the designated IAFIS repository as a result of an Evaluation Latent Fingerprint Submission Request.

3.4.14.3 Evaluation Latent Fingerprint Submission Request Outputs

FR507 IAFIS shall provide a response to an Evaluation Latent Fingerprint Submission request in accordance with the latest EFTS version.

IAFIS does not generate a response for Evaluation Latent Fingerprint Submission requests, other than a communication protocol level acknowledgement. The FBI Service Provider (Latent Examiner) who processes the transactions will be responsible for contacting the Authorized Contributor (FBI field office) with evaluation results.

3.5 Notification Services Functional Requirements

The Notification Service provides Authorized Contributors with unsolicited notifications from the system based on event criteria (triggers). An unsolicited notification may be triggered by functions initiated by the system, FBI Service Providers, or Authorized Contributors. The notifications to the users may be in multiple formats (i.e., electronic, telephonic, hardcopy, etc.).

The following section contains the functional requirements supporting Notification user services.

3.5.1 Flash Notifications

A Flash Notification will be provided to an Authorized Contributor when criminal activity or file maintenance occurs on a subject's record containing a Flash for that Contributor. Flashes may be placed on records for a subject whose activities are limited by court issued restrictions, supervision, protection orders, or deportation decrees.

FR242 IAFIS shall notify an Authorized Contributor when criminal activity occurs on a subject's record containing a Flash for that Contributor.

FR243 IAFIS shall notify an Authorized Contributor when file maintenance occurs on a subject's record containing a Flash for that Contributor.

NGI-567

FR244 IAFIS shall generate a hardcopy Subject Criminal History Rap Sheet for a Flash Notification when appropriate.

3.5.2 Want Notifications

A Wanted Persons Notification will be provided to an Authorized Contributor when activity or file maintenance occurs on a subject's record containing a Want Notice for that Contributor. Wants are placed on a subject when a Wanted Person is entered into NCIC with valid FBI Number. An FBI Service Provider may also place wants on a subject's record on behalf of an Authorized Contributor.

FR245 IAFIS shall notify an Authorized Contributor when activity occurs on a subject's record containing a Want for that Contributor.

FR246 IAFIS shall notify an Authorized Contributor when file maintenance occurs on a subject's record containing a Want for that Contributor.

FR247 IAFIS shall generate a hardcopy Subject Criminal History Rap Sheet for a Want Notification when appropriate.

FR521 IAFIS shall send a Want Notification to an Authorized Contributor when their identification search results in a positive identification to a record containing a want.

FR248 IAFIS shall provide a Want Notification in accordance with the latest Nlets Operating Manual.

3.5.3 Sexual Offender Registry Notifications

IAFIS will notify the original registering agency of activity on criminal subject records that contain Sexual Offender Registry (SOR) data. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, expungement of last cycle), IAFIS will send a notice to each registering agency.

FR249 IAFIS shall notify an Authorized Contributor when criminal activity occurs on a subject's record containing Sexual Offender Registry data for that Contributor.

FR250 IAFIS shall notify an Authorized Contributor when file maintenance occurs on a subject's record containing Sexual Offender Registry data for that Contributor.

FR251 IAFIS shall provide Sexual Offender Registry Notification in accordance with the latest Nlets Operating Manual.

3.5.4 Other Special Interest Subject Notifications

IAFIS will notify the appropriate agency of activity on subjects of Special Interest. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, expungement of last cycle), IAFIS will send a notice to the appropriate agency.

FR252 IAFIS shall provide Special Interest Notification to an Authorized FBI Service Provider.

FR253 IAFIS shall provide Special Interest Notification to an Authorized Contributor in accordance with the latest III/NFF Operations and Technical Manual.

FR254 IAFIS shall provide Special Interest Notifications to external systems when appropriate

FR255 IAFIS shall generate a Special Interest Notification when criminal activity occurs on a subject's record marked as Special Interest.

FR256 IAFIS shall generate a Special Interest Notification when file maintenance occurs on a subject's record marked as Special Interest.

FR257 IAFIS shall generate a hardcopy Special Interest Notification when appropriate.

3.5.5 III/NFF File Maintenance Notifications

A State Bureau for a III/NFF state will be notified when file maintenance activities (e.g., posting an arrest, consolidating records or expungement of last cycle) occur against a record they own within IAFIS. Additionally, a III/NFF State Bureau will be notified of the search and record status resulting from a Ten-Print Fingerprint Identification Search submitted by an Authorized Contributor within their state.

FR258 IAFIS shall provide a File Maintenance Notification to an Authorized Contributor in accordance with the latest III/NFF Operations and Technical Manual.

FR259 IAFIS shall send a File Maintenance Notification to the III/NFF State Bureau when file maintenance activity occurs on a record owned by that State Bureau.

FR260 IAFIS shall send a File Maintenance Notification to the III/NFF State Bureau, when appropriate, indicating the search and record status resulting from of a Ten-Print Fingerprint Identification Search.

3.5.6 Unsolved Latent Match Notifications

The Unsolved Latent Match Notification informs the Unsolved Latent File (ULF) record owner that a potential match has occurred as a result of a Cascaded Fingerprint Search from a fingerprint transaction.

FR261 IAFIS shall notify the owner of an unsolved latent print that a potential match has resulted from a Cascaded Fingerprint Search.

FR262 IAFIS shall provide an Unsolved Latent Match Notification to an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Unsolved Latent Match Notification is ULM.

FR263 IAFIS shall provide an Unsolved Latent Match Notification to an Authorized Service Provider when appropriate.

The IAFIS STOT that supports the Unsolved Latent Match Notification is ULM.

3.5.7 Unsolicited Unsolved Latent Record Delete Notifications

The Unsolicited Unsolved Latent Record Delete Notification informs the Unsolved Latent File (ULF) record owner that their record has been deleted due to ULF reaching maximum capacity.

FR264 IAFIS shall notify the owner of an unsolved latent print that their record was deleted as a result of ULF reaching maximum capacity resulting from an add to the ULF.

FR265 IAFIS shall provide an Unsolicited Unsolved Latent Record Delete Notification to an Authorized Contributor in accordance with the latest EFTS version.

FR266 IAFIS shall provide an Unsolicited Unsolved Latent Record Delete Notification to an Authorized Service Provider when appropriate.

3.5.8 Shared Data Notification

The Shared Data Notification Service provides Authorized Contributors with unsolicited notifications on event criteria (triggers). Shared Data Notifications are unsolicited messages between IAFIS (iDSM) and the IDENT system notifying the other agency of a positive identification.

FR601 IAFIS shall send a Shared Data Hit Notification to IDENT when there is a positive identification against an image contained in the IDENT shared data as a result of an IAFIS Ten-Print Identification Search request from an Authorized iDSM Pilot Agency.

FR602 IAFIS shall include in the Shared Data Hit Notification to IDENT the associated IAFIS submission type (e.g., criminal arrest, civil application) that resulted in a positive identification against the IDENT shared data.

FR603 IAFIS shall include in the Shared Data Hit Notification to IDENT the associated Pilot Site Identifier for any IAFIS Ten-Print Identification Search request of the IDENT shared data resulting in a positive identification.

FR604 IAFIS shall accept a Shared Data Hit Notification from IDENT when there is a positive identification of a fingerprint submission against an image contained in the IAFIS Shared Data.

FR605 IAFIS shall accept as part of a Shared Data Hit Notification the reason for the IDENT submission type (e.g., Port of Entry (POE), Customs and Border Protection (CBP), Visa, Latent Search) that resulted in a positive identification.

3.6 Data Management Service Functional Requirements

The following section contains the functional requirements supporting Data Management user services.

3.6.1 Fingerprint Image Replacement Request

A Fingerprint Image Replacement Request is a full replacement of composite fingerprint images and features. This service is only available for the Criminal Master File.

3.6.1.1 Fingerprint Image Replacement Request Inputs

FR267 IAFIS shall accept Fingerprint Image Replacement Requests from Authorized Contributors in accordance with the latest EFTS version.

The EFTS TOT that supports the Fingerprint Image Replacement Request is FIS.

FR268 IAFIS shall allow an Authorized FBI Service Provider to submit a Fingerprint Image Replacement Request.

The internal STOT that supports the Fingerprint Image Replacement Request is IFIS.

FR269 IAFIS shall require Ten-Print fingerprint images and an FNU as part of a Fingerprint Image Replacement Request.

3.6.1.2 Fingerprint Image Replacement Request Processing

FR270 IAFIS shall retrieve the fingerprint images associated with the specified FNU as part of a Fingerprint Image Replacement Request.

FR271 IAFIS shall reject the Fingerprint Image Replacement Request when the specified FNU is invalid.

FR272 IAFIS shall require two Authorized FBI Service Providers to perform manual FICs for a Fingerprint Image Replacement Request.

FR273 IAFIS shall allow an Authorized FBI Service Provider to reject a Fingerprint Image Replacement Request as a result of the manual FIC.

FR274 IAFIS shall replace fingerprint images associated with the specified FNU using the fingerprint images provided in the Fingerprint Image Replacement Request.

FR275 IAFIS shall perform a cascaded fingerprint search of the ULF when the composite fingerprint images are updated.

3.6.1.3 Fingerprint Image Replacement Request Outputs

FR276 IAFIS shall provide a response to a Fingerprint Image Replacement Request in accordance with the latest EFTS version.

FR515 IAFIS shall provide the appropriate Fingerprint Image Replacement Request response to an Authorized FBI Service Provider.

3.6.2 Subject Criminal History Record Modification Request

Subject Criminal History (SCH) Record Modification (SCHMOD) Request provides the capabilities for an Authorized Service Provider to modify subject criminal history information. This capability will

allow the addition, modification, and deletion of selected data elements.

3.6.2.1 Subject Criminal History Record Modification Request Inputs

FR277 IAFIS shall allow an Authorized FBI Service Provider to submit a Subject Criminal History Record Modification Request.

The internal STOT that supports the Subject Criminal History Record Modification Requests is SCHD.

FR278 IAFIS shall require a subject identifier as part of a Subject Criminal History Record Modification Request.

FR279 IAFIS shall accept a designation of maintenance action as part of a Subject Criminal History Record Modification Request.

Maintenance actions may include addition, modifications, or deletions of individual SCH data elements or criminal history events. The maintenance action may also indicate deletion of entire SCH records.

3.6.2.2 Subject Criminal History Record Modification Request Processing

FR280 IAFIS shall perform the designated maintenance action on the specified subject's criminal history record as part of the Subject Criminal History Record Modification Request.

FR281 IAFIS shall reject the Subject Criminal History Record Modification Request when specified subject identifier is invalid.

3.6.2.3 Subject Criminal History (SCH) Record Modification Request Outputs

FR282 IAFIS shall provide the appropriate Subject Criminal History Record Modification Request response to an Authorized FBI Service Provider.

3.6.3 III Record Maintenance Request

III Record Maintenance Request provides the capabilities for an Authorized Contributor to modify subject criminal history information. This capability will allow the addition, modification, and deletion of selected data elements.

3.6.3.1 III Record Maintenance Request Inputs

FR283 IAFIS shall accept a III Record Maintenance Request from an Authorized Contributor in accordance with the III/NFF Operations and Technical Manual.

The III Message Keys (MKE) that support the SCH Record Modification Requests are: MRS, EHN, and XHN.

FR284 IAFIS shall require a subject identifier as part of a III Record Maintenance Request.

FR285 IAFIS shall allow an Authorized Contributor to add supplemental SCH biographic identifiers as part of a III Record Maintenance Request.

This supports the EHN III message.

FR286 IAFIS shall allow an Authorized Contributor to delete supplemental SCH biographic identifiers as part of a III Record Maintenance Request.

This supports the XHN III message.

FR287 IAFIS shall allow an Authorized Contributor to modify III Pointer data as part of a III Record Maintenance Request.

This supports the MRS III message.

3.6.3.2 III Record Maintenance Request Processing

FR288 IAFIS shall perform the designated maintenance action on the specified subject's criminal history record as part of the III Record Maintenance Request.

FR289 IAFIS shall reject the III Record Maintenance Request when specified subject identifier is invalid.

3.6.3.3 III Record Maintenance Request Outputs

FR290 IAFIS shall provide the appropriate III Record Maintenance Request response to an Authorized Contributor in accordance with the III/NFF Operations and Technical Manual.

3.6.4 Special Stops Maintenance Request

The Special Stops Maintenance Requests provides the capability for an Authorized Service Provider to change SCH record status or permissions. This capability also allows an Authorized Service Provider to create SCH records with or without associated fingerprint image data.

3.6.4.1 Special Stops Maintenance Request Inputs

FR291 IAFIS shall allow an Authorized Service Provider to submit a Special Stops Maintenance Request.

The internal STOT that supports the Special Stops Maintenance Request is SSMD.

FR292 IAFIS shall accept a subject identifier as part of a Special Stops Maintenance Request.

FR293 IAFIS shall accept fingerprint image data as part of a Special Stops Maintenance Request.

FR294 IAFIS shall accept a designation of maintenance action as part of a Special Stops Maintenance Request.

Maintenance actions may include addition, modifications, or deletions of audit (AUD) codes and Special Processing Flags (SPFs). Special Stops Maintenance actions will include modifying AUD Codes (i.e., AUD T to AUD P, AUD P to AUD T), addition/modification/deletion of SPF values, or creation of

records.

FR295 IAFIS shall allow an Authorized FBI Service Provider to scan fingerprint images as part of a Special Stops Maintenance Request when applicable.

The modification of a records AUD code from AUD T to AUD P will require the scanning of fingerprints.

3.6.4.2 Special Stops Maintenance Request Processing

FR296 IAFIS shall perform the designated maintenance action on the specified subject's criminal history record as part of the Special Stops Maintenance Request.

FR297 IAFIS shall reject the Special Stops Maintenance Request when specified subject identifier is invalid.

3.6.4.3 Special Stops Maintenance Request Outputs

FR298 IAFIS shall provide the appropriate Special Stops Maintenance Request response to an Authorized FBI Service Provider.

3.6.5 Master SCH Record Conversion Request

Master SCH Record Conversion Request provides capability for Authorized Service Provider to add event and corresponding fingerprint image data to an existing SCH record marked as a manual record.

3.6.5.1 Master SCH Record Conversion Request Inputs

FR299 IAFIS shall allow an Authorized FBI Service Provider to submit a Master SCH Record Conversion Request.

The internal STOT that supports the Master SCH Record Conversion Request is MRCD.

FR300 IAFIS shall require a subject identifier as part of a Master SCH Record Conversion Request.

FR301 IAFIS shall require criminal history event information as part of a Master SCH Record Conversion Request.

3.6.5.2 Master SCH Record Conversion Request Processing

FR302 IAFIS shall associate fingerprint image data and criminal history event information to the specified subject identifier's SCH record as part of Master SCH Record Conversion Request.

FR303 IAFIS shall reject the Master SCH Record Conversion Request when specified subject identifier is invalid.

3.6.5.3 Master SCH Record Conversion Request Outputs

FR304 IAFIS shall provide the appropriate Master SCH Record Conversion Request response to an Authorized FBI Service Provider.

3.6.6 Disposition Submission

The Disposition Submission service updates a criminal history record by associating court and custody information to an arrest cycle. Disposition processing submissions may be on paper or machine readable data (MRD) media.

3.6.6.1 Disposition Submission Inputs

FR668 IAFIS shall accept Disposition Submission requests from Authorized Contributors in accordance with the EFTS.

The STOT that supports the external Disposition Submission request is DSP.

FR305 IAFIS shall accept Disposition Submission request from Authorized Contributors in accordance with the MRD Disposition Manual.

The internal STOT that supports the MRD Disposition Submission requests is DSPM.

FR306 IAFIS shall allow an Authorized FBI Service Provider to submit a Disposition Submission request.

The internal STOT that supports the FBI Service Provider submitted Disposition Submission request is DSPD.

FR307 IAFIS shall require an FNU and Date of Arrest as part of a Disposition Submission request submitted by an Authorized FBI Service Provider.

3.6.6.2 Disposition Submission Processing

FR308 IAFIS shall update the Criminal History record for the associated FNU and Date of Arrest using the data provided in the Disposition Submission request.

FR309 IAFIS shall reject a Disposition Submission request submitted by an Authorized FBI Service Provider when the specified FNU is invalid.

FR310 IAFIS shall reject a Disposition Submission request when the specified DOA is invalid.

FR669 IAFIS shall allow an FBI Service Provider to manually resolve Disposition Submission discrepancies as part of conflict Resolution.

FR670 IAFIS shall defer a Disposition Submission when the disposition data cannot automatically be applied as part of conflict resolution.

3.6.6.3 Disposition Submission Outputs

FR311 IAFIS shall provide an MRD response to a Disposition Submission request in accordance with the MRD Disposition Manual.

FR509 IAFIS shall provide the appropriate Disposition Submission response to an Authorized FBI Service Provider.

FR671 IAFIS shall respond to a Disposition Submission from an authorized contributor request within 24 hours after the request is received.

3.6.7 Expungement Submission

The Expungement Submission request removes criminal history data for a specified arrest. Specific charges may be expunged from an arrest, or an entire arrest may be expunged. If the last arrest on a criminal history record is expunged, then the entire record will be expunged. Expungement Submissions may be hardcopy, electronic or machine readable data (MRD) media.

3.6.7.1 Expungement Submission Inputs

FR312 IAFIS shall accept electronic Expungement Submission requests from Authorized Contributors in accordance with the III Operation and Technical Manual.

The III Message Key (MKE) that supports the Expungement Submission requests is DRS.

FR313 IAFIS shall accept Expungement Submission requests from Authorized Contributors in accordance with the MRD Expungement Manual.

The internal STOT that supports the MRD Expungement Submission requests is EXPM.

FR314 IAFIS shall allow an Authorized FBI Service Provider to submit an Expungement Submission request.

The internal STOTs that support the FBI Service Provider submitted Expungement Submission request are EXPD and PEXD.

FR315 IAFIS shall require an FNU and Date of Arrest as part of an Expungement Submission request.

3.6.7.2 Expungement Submission Processing

FR316 IAFIS shall expunge the arrest data and appropriate criminal history information associated with the FNU and Date of Arrest provided in the Expungement Submission request.

FR317 IAFIS shall reject an Expungement Submission request when the specified FNU is invalid.

FR318 IAFIS shall reject an Expungement Submission request when the specified DOA is invalid.

3.6.7.3 Expungement Submission Outputs

FR319 IAFIS shall provide an MRD response to an Expungement Submission request in accordance with the MRD Expungement Manual.

FR320 IAFIS shall provide an electronic response to an Expungement Submission request in accordance with the III/NFF Operations and Technical Manual.

FR321 IAFIS shall provide a hardcopy of criminal history information in response to an Expungement Submission Request, if appropriate.

FR510 IAFIS shall provide the appropriate Expungement Submission response to an Authorized FBI Service Provider.

3.6.8 Criminal Record Sealing Request

Criminal Record Sealing Request allows an Authorized Contributor to restrict the access of the criminal history information associated with arrests that they own. The FBI will limit dissemination of criminal history data related to a sealed criminal arrest record. A III Message Key EHN allows an NFF Authorized Contributor to "seal" the pointer to a specified state controlled record. An FBI Service Provider can "seal" individual arrest records on behalf of an Authorized Contributor.

3.6.8.1 Criminal Record Sealing Request Inputs

FR322 IAFIS shall accept electronic Criminal Record Sealing Submission Requests from Authorized Contributors in accordance with the III Operation and Technical Manual.

The III Message Key (MKE) that supports the Criminal Record Sealing Submission Requests is EHN.

FR323 IAFIS shall allow an Authorized FBI Service Provider to submit a Criminal Record Sealing Request.

The internal STOT that supports the FBI Service Provider submitted Criminal Record Sealing Request is RSD.

FR324 IAFIS shall require a seal indicator designating whether specified criminal arrest record should be sealed or un-sealed as part of Criminal Record Sealing Request.

FR325 IAFIS shall require an FNU and arrest record specific information as part of a Criminal Record Sealing Request.

3.6.8.2 Criminal Record Sealing Request Processing

FR326 IAFIS shall seal a criminal arrest record and associated criminal history information when indicated in the Criminal Record Sealing Request.

FR327 IAFIS shall un-seal a criminal arrest record and associated criminal history information when indicated in the Criminal Record Sealing Request.

FR328 IAFIS shall reject a Criminal Record Sealing Request when the specified FNU is invalid.

NGI-577

FR329 IAFIS shall reject a Criminal Record Sealing Request when the specified arrest record information is invalid.

3.6.8.3 Criminal Record Sealing Request Outputs

FR330 IAFIS shall provide an electronic response to a Criminal Record Sealing Request in accordance with the III/NFF Operations and Technical Manual.

FR501 IAFIS shall provide the appropriate Criminal Record Sealing Request response to an Authorized FBI Service Provider.

3.6.9 Criminal Record Consolidation Request

A Criminal Record Consolidation Request will be initiated when multiple Subject Criminal History Records are found to exist for the same individual. A service provider will review the criminal fingerprint images and determine if the records should be consolidated. The Criminal Record Consolidation Request causes the information in the multiple records to be merged and the information associated with the secondary records to be deleted. As a result of the consolidation, a notification will be sent to the agency that submitted the fingerprints; any agencies that have submitted fingerprints pertinent to any of the records in the last year; and all state ID bureaus that have submitted fingerprints or records at any time on the consolidated subject.

3.6.9.1 Criminal Record Consolidation Request Inputs

FR331 IAFIS shall allow an Authorized FBI Service Provider to submit a Criminal Record Consolidation Request.

The internal STOT that supports the FBI Service Provider submitted Criminal Record Consolidation Request is COND.

FR332 IAFIS shall accept a Criminal Record Consolidation Request when a Ten-Print Fingerprint Identification Search results in multiple "Ident" decisions.

FR333 IAFIS shall require at least two FNUs as part of a Criminal Record Consolidation Request.

3.6.9.2 Criminal Record Consolidation Request Processing

FR334 IAFIS shall determine "kept FNU" (FBK) and "killed FNU(s)" from the FNUs provided as part of a Criminal Record Consolidation Request based on consolidation rule.

FR335 IAFIS shall allow IAFIS Service Providers to determine "kept FNU" (FBK) and "killed FNU(s)" from the FNUs provided as part of a Criminal Record Consolidation Request.

FR336 IAFIS shall perform Automated Consolidation of the criminal history information associated with the "killed FNU(s)" into the "kept FNU" (FBK) provided as part of the Criminal Record Consolidation Request.

FR337 IAFIS shall allow an Authorized FBI Service Provider to perform Manual Consolidation when Automated Consolidation cannot be successfully completed as part of the Criminal Record Consolidation Request.

FR338 IAFIS shall reject a Criminal Record Consolidation Request when the fingerprints for the FNUs are determined to not be the same individual.

FR339 IAFIS shall reject a Criminal Record Consolidation Request when record types for the submitted FNUs are not compatible.

3.6.9.3 Criminal Record Consolidation Request Outputs

FR511 IAFIS shall provide the appropriate Criminal Record Consolidation request response to an Authorized FBI Service Provider.

Criminal Record Consolidation Requests result in unsolicited notifications to the appropriate Authorized Contributors. Ten-Print Fingerprint Identification requests that trigger a Consolidation Request will resume normal processing after consolidation activities are completed. Refer to the *Notification Services Functional Requirements* section for more information.

FR581 IAFIS shall provide hardcopy Rap Sheets to each contributor that provided or received criminal history information for the kept FNU during the last 12-month time period.

3.6.10 Death Notice Request

Notification of the death of a subject may be received over NCIC. When a notice is received without a supporting fingerprint card, IAFIS maintains the status of "notice of death received" on the subject's record. When a death notice contains a supporting fingerprint card (refer to Ten-Print Fingerprint Identification Search request), the record is updated with a "deceased" status.

3.6.10.1 Death Notice Request Inputs

FR340 IAFIS shall accept a Death Notice Request in accordance with the III/NFF Operations and Technical Manual.

The III Message Key (MKE) that supports the Death Notice Request is DEC.

FR341 Deleted.

FR342 IAFIS shall require a FNU in a Death Notice Request.

3.6.10.2 Death Notice Request Processing

FR343 IAFIS shall update the specified FNU with information provided in a Death Notice Request.

FR344 IAFIS shall reject a Death Notice Request when the FNU is invalid.

3.6.10.3 Death Notice Request Outputs

FR345 IAFIS shall provide a response to a Death Notice Request in accordance with the III/NFF Operations and Technical Manual.

3.6.11 Want Maintenance Request

Electronic Want Maintenance Requests are received from NCIC when wanted person information is added, modified or deleted within the NCIC wanted person file, and there is an FNU associated with the record. If IAFIS cannot automatically process the electronic Want Maintenance Request, a reject message is printed for an Authorized FBI Service Provider to review. Additionally, FBI Service Providers have the capability to manually submit Want Maintenance Requests.

3.6.11.1 Want Maintenance Request Inputs

FR346 IAFIS shall accept Want Maintenance Requests from NCIC in accordance with the latest NCIC Operating Manual.

The internal STOT that supports the Want Maintenance Request is WPT.

FR347 IAFIS shall allow an Authorized FBI Service Provider to submit a Want Maintenance Request.

The internal STOT that supports the FBI Service Provider submitted Want Maintenance Requests is WPTD.

FR348 IAFIS shall require an FNU and biographical data as part of a Want Maintenance Request.

FR349 IAFIS shall require a designation of file maintenance type (e.g. add, modify, delete) as part of a Want Maintenance Request.

3.6.11.2 Want Maintenance Request Processing

FR350 IAFIS shall perform biographic validation using FNU and biographic data to validate the subject associated with the Want Maintenance Request.

FR351 IAFIS shall update the Criminal History record for the associated FNU using the designated file maintenance type and other data contained in the Want Maintenance Request.

FR352 IAFIS shall reject a Want Maintenance Request when the specified FNU is invalid.

FR353 IAFIS shall reject a Want Maintenance Request when biographic validation fails.

3.6.11.3 Want Maintenance Request Outputs

IAFIS does not provide any response when a WANT Maintenance Request completes successfully.

NGI-580

FR354 IAFIS shall generate a hardcopy reject in response to a Want Maintenance Request, when appropriate.

FR522 IAFIS shall provide the appropriate Want Maintenance Request response to an Authorized FBI Service Provider.

If appropriate, IAFIS will also send unsolicited notifications to Authorized Contributors.

3.6.12 Flash Submission

Flashes may be placed on records for a subject whose activities are limited by court issued restrictions, supervision, protection orders, or deportation decrees.

3.6.12.1 Flash Submission Inputs

FR355 IAFIS shall allow an Authorized FBI Service Provider to submit a Flash Submission.

The internal STOT that supports the FBI Service Provider Flash Submission is FLASH.

FR356 IAFIS shall require an FNU and Date of Arrest (DOA) as part of a Flash Submission.

3.6.12.2 Flash Submission Processing

FR357 IAFIS shall update the Criminal History record for the associated FNU and DOA using the information contained in the Flash Submission.

FR358 IAFIS shall reject a Flash Submission when the specified FNU is invalid.

FR359 IAFIS shall reject a Flash Submission when the specified DOA is invalid.

3.6.12.3 Flash Submission Request Outputs

FR512 IAFIS shall provide the appropriate Flash Submission response to an Authorized FBI Service Provider.

FR360 IAFIS shall generate a hardcopy response to a Flash Submissions, if appropriate.

If appropriate, IAFIS will also send unsolicited notifications to Authorized Contributors.

3.6.13 Sexual Offender Registry (SOR) Maintenance Request

Electronic SOR Maintenance Requests are received from NCIC when sexual offender information is added, modified or deleted within the NCIC sexual offender file, and there is an FNU associated with the record. If IAFIS cannot automatically process the electronic Sexual Offender Registry Maintenance Request, a reject message is printed for an Authorized FBI Service Provider to review.

3.6.13.1 SOR Maintenance Request Inputs

FR361 IAFIS shall accept SOR Maintenance Requests from NCIC in accordance with the latest NCIC Operating Manual.

The internal STOT that supports the Want Maintenance Request is WPT.

FR362 IAFIS shall require an FNU and biographical data as part of an SOR Maintenance Request.

FR363 IAFIS shall require a designation of file maintenance type (e.g. add, modify, delete) as part of an SOR Maintenance Request.

3.6.13.2 SOR Maintenance Request Processing

FR364 IAFIS shall perform biographic validation using FNU and biographic data to validate the subject associated with the SOR Maintenance Request.

FR365 IAFIS shall update the Criminal History record for the associated FNU using the designated file maintenance type and other data contained in the SOR Maintenance Request.

FR366 IAFIS shall reject an SOR Maintenance Request when the specified FNU is invalid.

FR367 IAFIS shall reject an SOR Maintenance Request when biographic validation fails.

3.6.13.3 SOR Maintenance Request Outputs

FR368 IAFIS shall generate a hardcopy reject in response to an SOR Maintenance Request, when appropriate.

If appropriate, IAFIS will also send unsolicited notifications to Authorized Contributors.

3.6.14 Photo Maintenance Request

3.6.14.1 Photo Image Delete Request Inputs

FR369 IAFIS shall accept Photo Image Delete Requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Photo Image Delete Requests is CPD.

FR370 IAFIS shall require FNU and Date of Arrest (DOA) as part of a Photo Image Delete Requests.

3.6.14.2 Photo Image Delete Request Processing

FR371 IAFIS shall delete the photo set associated with the FNU and Date of Arrest (DOA) provided as part of a Photo Image Delete Request.

FR372 IAFIS shall reject a Photo Image Delete Request when the specified FNU is invalid.

FR373 IAFIS shall reject a Photo Image Delete Request when the specified DOA is invalid.

NGI-582

FR583 IAFIS shall reject a Photo Image Delete Request when the Contributor of the request is not the owner of the photo set.

3.6.14.3 Photo Image Delete Request Outputs

FR374 IAFIS shall provide a response to a Photo Image Delete Request in accordance with the latest EFTS version.

3.6.15 Unsolved Latent File (ULF) Delete Request

The Unsolved Latent File Delete Request provides the capability for a ULF record owner to delete a latent print from the ULF.

3.6.15.1 ULF Delete Request Inputs

FR375 IAFIS shall accept Unsolved Latent File Delete Requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Unsolved Latent File Delete requests is ULD.

FR376 IAFIS shall allow an Authorized FBI Service Provider to submit an Unsolved Latent File Delete Request.

The IAFIS STOT that supports the Unsolved Latent File Delete request is IULD.

FR377 IAFIS shall require a unique identifier as part of an Unsolved Latent File Delete Request.

3.6.15.2 ULF Delete Request Processing

FR378 IAFIS shall reject an Unsolved Latent File Delete Request when the specified unique identifier does not exist.

FR379 IAFIS shall delete the fingerprint data from the Unsolved Latent File associated with the unique identifier specified in the Unsolved Latent File Delete Request.

FR582 IAFIS shall reject an Unsolved Latent File Delete Request when the requestor is not the owner of the ULF record.

3.6.15.3 ULF Delete Request Outputs

FR380 IAFIS shall provide a response to a Unsolved Latent Delete Request in accordance with the latest EFTS version.

FR513 IAFIS shall provide the appropriate Unsolved Latent Delete Request response to an Authorized FBI Service Provider.

3.6.16 Special Latent Cognizant Maintenance Request

The Special Latent Cognizant Maintenance Request provides the capability for an Authorized Contributor or FBI Service Provider (Latent Examiner) to maintain (add/copy/delete) data for a Special

Latent Cognizant File.

3.6.16.1 Special Latent Cognizant Maintenance Request Inputs

FR502 Deleted.

FR381 IAFIS shall allow an Authorized Service Provider to submit a Special Latent Cognizant Maintenance Request.

The internal STOTs that support the Special Latent Cognizant Maintenance Requests are SLC and ISLC.

FR382 IAFIS shall require a SLC identifier as part of a Special Latent Cognizant Maintenance Request.

FR383 IAFIS shall accept a designation of maintenance action as part of a Special Latent Cognizant Maintenance Request.

Maintenance actions may include addition, deletions, or copying of data to a Special Latent Cognizant file.

3.6.16.2 Special Latent Cognizant Maintenance Request Processing

FR384 IAFIS shall perform the designated maintenance action on the specified Special Latent Cognizant File as part of the Special Latent Cognizant Maintenance Request.

FR385 IAFIS shall reject the Special Latent Cognizant Maintenance Request when specified SLC File is invalid.

3.6.16.3 Special Latent Cognizant Maintenance Request Outputs

FR386 IAFIS shall provide the appropriate Special Latent Cognizant Maintenance Request response to an Authorized Service Provider.

FR503 Deleted.

3.6.17 Computerized Contributor Address (CCA) File Maintenance Request

3.6.17.1 Computerized Contributor Address File Maintenance Request Inputs

FR387 IAFIS shall allow Authorized FBI Service Provider to submit a CCA File Maintenance Request.

The internal STOT that supports the CCA File Maintenance is CCAD.

FR388 IAFIS shall accept from an Authorized FBI Service Provider the designation to add a Contributor Address record as part of a CCA File Maintenance Request.

FR389 IAFIS shall accept from an Authorized FBI Service Provider the designation to deactivate (retire) a Contributor Address record in the CCA File as part of a CCA File Maintenance Request.

NGI-584

The association of deactivated Contributor entries to another active Contributor entry allows changes in contributor identifiers (ORIs) due to policy, business rules, and programmatic changes.

FR390 IAFIS shall accept from an Authorized FBI Service Provider a designation of data maintenance action as part of a CCA File Maintenance Request.

Data maintenance actions may include addition, modifications, or deletions of CCA data.

3.6.17.2 Computerized Contributor Address File Maintenance Request Processing

FR391 IAFIS shall create a record in the CCA File based on Contributor Address data provided as part of a add contributor CCA File Maintenance Request.

FR508 IAFIS shall discontinue (retire) a Contributor's Address record based on information provided by a FBI Service Provider as part of a deactivate contributor CCA File Maintenance Request.

FR392 IAFIS shall associate discontinue (retire) a Contributor's Address record to another active Contributor Address record based on information provided by FBI Service Provider as part of a deactivate contributor CCA File Maintenance Request.

There will be instances where a Contributor's agency or organizational structure changes requiring the consolidation of points of contact with the FBI. The deactivated points of contact (contributor address) will need to be associated with the new or other existing Contributor Address information to facilitate inquiries and reporting of past events.

FR393 IAFIS shall perform the designated maintenance action on the specified Contributor Address record data as part of the CCA File Maintenance Request.

3.6.17.3 Computerized Contributor Address File Maintenance Request Outputs

FR394 IAFIS shall provide the appropriate CCA File Maintenance Request response to an Authorized Service Provider.

3.6.18 Restore Subject Criminal History Information Request

3.6.18.1 Restore Subject Criminal History Information Request Inputs

FR395 IAFIS shall allow an Authorized FBI Service Provider to submit a Restore Subject Criminal History Record Request.

The IAFIS STOT that supports the Restore FNU request is RFND.

FR396 IAFIS shall accept from an Authorized FBI Service Provider a FNU as part of a Restore Subject Criminal History Record Request.

3.6.18.2 Restore Subject Criminal History Information Request Processing

FR397 IAFIS shall restore the criminal history information of the subject contained in a Restore Subject Criminal History Information Request within a specified period of time following a record expungement action.

FR398 IAFIS shall restore the criminal history information of the subject contained in within a Restore Subject Criminal History Information Request within a specified period of time following a record consolidation action.

FR399 IAFIS shall restore the criminal history information of the subject contained in within a Restore Subject Criminal History Information Request within a specified period of time following a record SCH record deletion action.

FR400 IAFIS shall reject a Restore Subject Criminal History Information Request when the specified FNU is invalid.

3.6.18.3 Restore Subject Criminal History Information Request Outputs

FR401 IAFIS shall provide the appropriate Restore Subject Criminal History Information Request response to an Authorized Service Provider.

IAFIS may also send unsolicited notifications to Authorized Contributors (e.g., III/NFF record owners, latent owners).

3.6.19 NFF Criminal Print Ident Notification

3.6.19.1 NFF Criminal Print Ident Notification Inputs

FR523 IAFIS shall accept an NFF Criminal Print Ident Notification from an NFF State in accordance with the III/NFF Operations and Technical Manual.

The IAFIS STOT that supports the NCIC MKE NFF Criminal Print Ident Notification is CPI.

FR524 IAFIS shall require a FNU and SID as part of the NFF Criminal Print Ident Notification.

3.6.19.2 NFF Criminal Print Ident Notification Processing

FR526 IAFIS shall validate FNU and SID included in the NFF Criminal Print Ident Notification prior to generating notifications to Authorized Contributors (e.g., Wanting Agency).

NFF Criminal Print Ident Notification results in unsolicited notifications to the appropriate Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.19.3 NFF Criminal Print Ident Notification Outputs

FR525 IAFIS shall provide an NFF Criminal Print Ident Notification response to an NFF State in accordance with III/NFF Operations and Technical Manual.

3.6.20 Statute Retrieval Requests

The purpose of the IAFIS Statute Retrieval request is to allow an Authorized FBI Service Provider to retrieve statutes for viewing or printing.

3.6.20.1 Statute Retrieval Request Inputs

FR533 IAFIS shall allow an Authorized FBI Service Provider to submit Statute Retrieval requests in support of AQC.

FR534 IAFIS shall require either a State code or a CRI in a Statute Retrieval request.

3.6.20.2 Statute Retrieval Request Processing

FR535 IAFIS shall retrieve the statute(s) for the State code or CRI indicated in the Statute Retrieval request.

3.6.20.3 Statute Retrieval Request Outputs

FR536 IAFIS shall provide the capability for an Authorized FBI Service Provider to view the statute(s) returned from a Statute Retrieval request.

FR537 IAFIS shall provide the capability for an Authorized FBI Service Provider to print the statute(s) returned from a Statute Retrieval request.

3.6.21 Statute Maintenance Request

The purpose of the IAFIS Statute Maintenance request is for an Authorized FBI Service Provider to perform statute maintenance. Once the necessary information is received to initiate a statute maintenance action, an Authorized FBI Service Provider can add, modify or delete a statute and IAFIS will maintain a statute maintenance audit trail for each transaction. *(text modified)*

3.6.21.1 Statute Maintenance Request Inputs

FR538 IAFIS shall allow an Authorized FBI Service Provider to submit Statute Maintenance requests in support of AQC.

FR539 IAFIS shall require a designation of file maintenance type (e.g., add, modify, delete) as part of a Statute Maintenance request.

3.6.21.2 Statute Maintenance Request Processing

FR540 IAFIS shall perform the appropriate file maintenance for the statute as indicated in the Statute Maintenance request.

3.6.21.3 Statute Maintenance Request Outputs

FR541 IAFIS shall provide the appropriate response to an Authorized FBI Service Provider for a Statute Maintenance request.

3.6.22 Unsolved Latent Add Confirm Request

This request is used to confirm temporarily added unsolved latent file records.

3.6.22.1 Unsolved Latent Add Confirm Inputs

FR562 IAFIS shall accept Unsolved Latent Add Confirm Requests from an Authorized Contributor in accordance with the latest EFTS version.

The EFTS TOT that supports the Unsolved Latent File Add Confirm request is ULAC.

FR563 IAFIS shall allow an Authorized FBI Service Provider to submit an Unsolved Latent Add Confirm request.

The IAFIS STOT that supports the Unsolved Latent File Add Confirm request is IULAC.

FR564 IAFIS shall require an AFIS segment process control number (SCNA) as part of an Unsolved Latent Add Confirm request.

FR565 IAFIS shall accept a Latent Case Number (LCN) and Latent Case Extension Number (LCX) as part of an Unsolved Latent Add Confirm request.

3.6.22.2 Unsolved Latent Add Confirm Processing

FR566 IAFIS shall mark the appropriate ULF image record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

FR567 IAFIS shall mark the appropriate ULF feature record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

3.6.22.3 Unsolved Latent Add Confirm Outputs

FR568 IAFIS shall provide an appropriate response to the Unsolved Latent Add Confirm Request in accordance with the latest EFTS version.

FR569 IAFIS shall provide the appropriate Unsolved Latent Add Confirm Request response to an Authorized FBI Service Provider.

3.6.23 Computerized Records Sent File Maintenance Request

The CRS database, maintained by III, contains records of those agencies that receive copies of responses.

3.6.23.1 Computerized Records Sent File Maintenance Request Inputs

FR570 IAFIS shall allow an Authorized FBI Service Provider to submit a Computerized Records Sent File Maintenance Request.

The internal STOT that supports the Computerized Records Sent File Maintenance Request is CRSD.

NGI-588

FR571 IAFIS shall require a subject identifier as part of a Computerized Records Sent File

Maintenance Request.

FR572 IAFIS shall accept a designation of maintenance action as part of a Computerized Records Sent File Maintenance Request.

3.6.23.2 Computerized Records Sent File Maintenance Request Processing

FR573 IAFIS shall provide the capability for an Authorized FBI Service Provider to access the Receiving Agency Notification Report (RANR) as part of a Computerized Records Sent File Maintenance Request.

FR574 IAFIS shall perform the designated maintenance action as part of a Computerized Records Sent File Maintenance Request.

FR575 IAFIS shall reject the Computerized Records Sent File Maintenance Request when the maintenance action is unsuccessful.

3.6.23.3 Computerized Records Sent File Maintenance Request Outputs

FR576 IAFIS shall provide the appropriate Computerized Records Sent File Maintenance Request response to an Authorized FBI Service Provider.

3.6.24 Shared Data Direct Enrollment

The following section contains the functional requirements that support the enrollment of records into the iDSM. The process of enrolling implies an add to the iDSM. The iDSM is comprised of the IAFIS Shared Want Files which contain IAFIS records and the DHS Shared Watch Files which contain IDENT records.

3.6.24.1 Inputs

FR606 IAFIS shall enroll IAFIS shared data that meets enrollment criteria (e.g., wants or warrants) into the Shared Data File on a periodic basis.

The IAFIS Shared Want File contains specific information of all individuals for which there is a want or warrant posted in the Subject Criminal History file and for which fingerprint images are available.

FR607 IAFIS shall retrieve the IAFIS images as part of an IAFIS shared data enrollment request.

FR608 IAFIS shall compress all images enrolled as part of an IAFIS shared data enrollment request in accordance with the latest version of the EFTS (e.g., using Wavelet Scalar Quantization (WSQ) at a ratio 15:1).

FR609 IAFIS shall include an FNU as part of an IAFIS shared data enrollment.

FR610 IAFIS shall include the subject's gender, name and date of birth (DOB) as part of an IAFIS shared data enrollment.

FR611 IAFIS shall accept shared data enrollment requests from IDENT in accordance with the latest version of the EFTS.

Enrollment requests from IDENT will be stored in the DHS Shared Watch file.

FR612 IAFIS shall accept two ANSI/NIST Type 4 image records from IDENT as part of a shared data enrollment request.

FR613 IAFIS shall accept 14 ANSI/NIST Type 4 image records from IDENT as part of a shared data enrollment request.

FR614 IAFIS shall be able to read the latest version of fingerprint images available for all individuals provided by IDENT as part of a shared data enrollment request.

FR615 IAFIS shall de-compress all fingerprint images in accordance with the latest version of the EFTS (e.g., using Wavelet Scalar Quantization (WSQ) at ratio 15:1) as part of a shared data enrollment request from IDENT.

3.6.24.2 Processing

FR616 IAFIS shall extract fingerprint features from the fingerprint images provided by IDENT as part of a shared data enrollment request.

FR617 IAFIS shall store in the shared data the extracted fingerprint features received as part of a shared data enrollment request from IDENT.

FR618 IAFIS shall remove fingerprint images received as part of a shared data enrollment request from IDENT within 24 hours following a successful features extraction.

FR619 IAFIS shall perform a Ten-Print Fingerprint Investigative Image Search (TPIS) as a result of a shared data enrollment request from IDENT.

FR620 IAFIS shall generate a list of candidates as the result of a Ten-Print Investigative Image Search initiated by a shared data enrollment request from IDENT.

FR621 IAFIS shall determine a "match score" for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT.

FR622 IAFIS shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as a result of a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT.

FR623 IAFIS shall require an Authorized FBI Service Provider to perform an iDSM manual image comparison for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT that is below the high confidence threshold.

FR624 IAFIS shall require a second Authorized FBI Service Provider to perform an iDSM manual image comparison to confirm a positive identification for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT that is below the low confidence threshold.

FR625 IAFIS shall store all candidates and their correlating EID resulting in a positive identification as a result of a Ten-Print Investigative Image Search initiated by a shared data enrollment request from IDENT.

IAFIS will maintain the FNUs and DHS unique id (EIDs) of all idented Shared Watch List Candidates.

3.6.24.3 Output

FR626 IAFIS shall reject a shared data enrollment request that fails to include a valid ORI.

FR627 Deleted.

FR628 IAFIS shall generate an Error Message to IDENT resulting from a failed shared data enrollment request from IDENT.

3.6.25 Shared Data Maintenance

Maintenance messages from IAFIS include removals and demotions. A demotion is a canceled Want in IAFIS that may be maintained in IDENT if a previous encounter has occurred. Maintenance messages from IDENT include only deletions.

3.6.25.1 Inputs

FR629 IAFIS shall process shared data removal requests for IAFIS Shared Data (e.g., wants or warrants) when indicated.

FR630 IAFIS shall process shared data demotion requests for IAFIS Shared Data (e.g., wants or warrants) when indicated.

FR631 IAFIS shall accept a shared data removal requests from IDENT in accordance with the latest version of the EFTS.

3.6.25.2 Processing

FR632 IAFIS shall remove all biometric and biographic information for individuals identified in a shared data removal request.

FR633 IAFIS shall remove all biometric and biographic information for individuals identified in a shared data demotion request.

FR634 IAFIS shall remove all biometric and biographic information for individuals identified in a shared data removal request from IDENT.

FR635 IAFIS shall identify the DHS unique identifier for any individual for whom the DHS received an order to remove or demote.

FR636 IAFIS shall be able to match the DHS unique identifier and the corresponding images for each individual provided by IDENT.

3.6.25.3 Outputs

FR637 IAFIS shall generate an Error Message for a failed shared data maintenance request of IAFIS Shared Data.

FR638 IAFIS shall generate an Error Message to IDENT resulting from a failed IDENT shared data maintenance request.

3.7 Administrative and Control Services

The following section contains those functional requirements that are related to specific areas of the administrative and control functions of the IAFIS.

3.7.1 System Status and Reporting (SSR)

The System Status and Reporting (SSR) capability provides status information on current response time performance, resources allocated to each environment (operational, testing, etc.), the readiness and availability of hardware components, staffing resources, and other information to identify processing bottlenecks and tune system performance.

FR402 IAFIS shall allow Authorized FBI System Administrators access to system status and reporting capabilities.

FR403 IAFIS shall collect system status data (i.e., readiness, utilization, queue status) for system components.

FR404 IAFIS shall collect system performance data (i.e., response times, workload).

FR405 IAFIS shall report system status information on each active system environment (i.e., operational, development support, and test support).

FR406 IAFIS shall report system performance information on each active system environment (i.e., operational, development support, and test support).

FR407 IAFIS shall retain system status data.

FR408 IAFIS shall retain system performance data.

FR639 IAFIS shall be capable of reporting the number of positive identifications resulting from searches against the IAFIS shared data.

FR640 IAFIS shall be capable of reporting the number of positive identifications resulting from searches against the IDENT shared data.

FR641 IAFIS shall be capable of reporting the number of fingerprint searches performed against the records contained in the IAFIS shared data.

FR642 IAFIS shall be capable of reporting the number of fingerprint searches performed against the records contained in the IDENT shared data.

3.7.2 Data Management

This section provides all functional requirements specific to the data management of the IAFIS.

3.7.2.1 IAFIS Access Authorization Rules

Access to IAFIS repository files will be controlled based on a set of authorization rules. IAFIS will provide the capability to add, delete and modify these authorization rules.

NGI-592

FR409 IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Subject Criminal History activities.

FR410 IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Fingerprint maintenance activities.

FR411 IAFIS shall maintain authorization rules (i.e., read/write/delete access) for all Latent maintenance activities.

FR412 IAFIS shall support FBI Service Provider workgroup assignments.

The IAFIS staffing workload will be distributed among organized workgroups, where feasible. The FBI will provide a work atmosphere that encourages the evolution of the self-directed workgroup.

3.7.2.2 IAFIS Dissemination Rules

FR413 IAFIS shall apply dissemination rules to all IAFIS notifications.

FR414 IAFIS shall apply dissemination rules to all IAFIS responses.

FR415 IAFIS shall maintain dissemination rules for all Subject Criminal History responses.

FR416 IAFIS shall maintain dissemination rules for all fingerprint responses.

FR417 IAFIS shall maintain dissemination rules for all Latent responses.

3.7.2.3 IAFIS Repository File Maintenance Rules

FR418 IAFIS shall perform maintenance of subject criminal history contained within the IAFIS Repositories as a result of fingerprint identification searches in accordance with Table 3-1: File Maintenance Rules.

FR419 IAFIS shall perform maintenance of fingerprint information contained within the IAFIS Repositories as a result of fingerprint identification searches in accordance with Table 3-1: File Maintenance Rules.

Table 3-1 File Maintenance Rules

Submission Type	Subject Criminal History File	Ten-Print Certification File	Criminal Ten-Print Images, & Features & Latent Cognizant	On-Line Civil File Image & On-Line Civil Subject Index	On-Line Civil Features
CRIMINAL					
Ident-Retain	Update	Add	Quality Improvement	N.A.	N.A.
Ident-Return	Update **	Add	Quality Improvement	N.A.	N.A.
Non-Ident—Retain	Add New	Add	Add New	N.A.	N.A.
Non-Ident- Return	No	No	NGI-593 No	N.A.	N.A.

Submission Type	Subject Criminal History File	Ten-Print Certification File	Criminal Ten-Print Images, & Features & Latent Cognizant	On-Line Civil File Image & On-Line Civil Subject Index	On-Line Civil Features
CIVIL (FEDERAL EMPLOYEE) vs. CRIMINAL FILE					
Ident-Retain	Update*	Add	Quality Improvement	No	No
Ident-Return	Update*	Add	Quality Improvement	No	No
Non-Ident—Retain	No	No	No	Add	Add
Non-Ident—Return	No	No	No	No	No
CIVIL (STATE/LOCAL) vs. CRIMINAL FILE					
Non-Ident—Return	No	No	No	No	No
Ident-Return	Update*	Add	Quality Improvement	No	No
Unknown Deceased, Missing Persons, Amnesia Victims and Living John Does Non-Ident—Retain/Return	Add New	Add	Add New	No	No
Unknown Deceased, Missing Persons, Amnesia Victims and Living John Does Ident - Retain/Return	Update*	Add	Quality Improvement	No	No

* For non-dissemination only. ** Juvenile records for non-dissemination only.

3.7.2.4 Subject Criminal History Rap Sheet

FR420 IAFIS shall provide an FNU as part of a Subject Criminal History Rap Sheet.

FR421 IAFIS shall provide biographic information as part of a Subject Criminal History Rap Sheet.

FR422 IAFIS shall provide event information as part of the Subject Criminal History Rap Sheet

Event information may be retained as part of a criminal juctice (e.g. notations of arrests, detention, criminal charges, and dispositions).

FR423 IAFIS shall provide active want information as part of the Subject Criminal History Rap Sheet.

FR424 IAFIS shall provide active Flash information as part of the Subject Criminal History Rap Sheet.

FR425 IAFIS shall provide active SOR information as part of the Subject Criminal History Rap Sheet.

3.7.2.5 Ten-Print Fingerprint Search Data Management

The following functional requirements are specific to the data management supporting Ten-Print Fingerprint Services:

FR426 IAFIS shall maintain business rules to support the Automated Quality Check (AQC) of textual data as part of a Ten-Print fingerprint Identification Search.

FR427 IAFIS shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint retention.

FR428 IAFIS shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint searches.

FR429 IAFIS shall maintain a minimum fingerprint match thresholds to support III/Verify function.

FR430 IAFIS shall support fingerprint image compression algorithm in accordance with the EFTS.

Once a ten-print image has been scanned into the system it will be compressed. All images will be transmitted in compressed format. Compression algorithm(s) used within IAFIS shall conform to the IAFIS Wavelet-Scalar Quantization (WSQ) Gray Scale Fingerprint Image Compression Specification referenced in the *Electronic Fingerprint Transmission Specification.*

FR431 IAFIS shall maintain a Fingerprint Image Compare (FIC) high confidence threshold to support automated Ten-Print Fingerprint Identification Search.

This threshold provides decision point for automated or "lights-out" identification decisions.

FR432 IAFIS shall maintain a Fingerprint Image Compare (FIC) low confidence threshold to support Ten-Print Fingerprint Identification Search.

This threshold provides decision point as to whether one or two manual FICs are required.

3.7.2.6 Latent Data Management

FR433 IAFIS shall delete the oldest record from the ULF, when ULF is at maximum capacity and a new record is received for enrollment.

FR584 IAFIS shall perform a comparison of stored latent investigative search results to produce a Post Latent Processing (PLP) Correlation List.

The PLP Correlation List will consist of FNUs or CRNs for the same candidate which appears in more than one set of search results for the same Latent Case (LCN).

FR585 IAFIS shall provide the capability to store latent search details.

3.7.2.7 Subject Criminal History Data Management

FR434 IAFIS shall provide the capability for storing multiple occurrences up to the maximum number of name, social security number, scars, marks, and tattoos, miscellaneous numbers, and dates of birth in each Subject Criminal History Record.

FR435 IAFIS shall support the synchronization of III subject criminal history data in accordance with the III/NFF Operations and Technical Manual.

A periodic III Subject Criminal History data synchronization will be conducted with state systems to ensure that data is consistent with the FBI systems. IAFIS data for specific states will be made available periodically via magnetic media or FTP for this synchronization process.

3.7.2.8 Shared Data Management

Maintenance of Shared Data business rules and thresholds allows for the modification of these parameters without impacting iDSM availability.

FR643 IAFIS shall provide the capability to maintain a shared data high confidence threshold to support automated comparison processes against candidates identified in a shared data search.

This threshold provides decision point for automated or "lights-out" identification or verification decisions.

FR644 IAFIS shall provide the capability to maintain a shared data low confidence threshold to support the automated comparison processes against candidates identified in a shared data search.

This threshold provides the decision point as to whether one or two manual FICs are required.

FR645 IAFIS shall provide the capability to maintain a daily IAQ search limit.

3.7.2.9 Computerized Contributor Address File (CCA) Maintenance

FR436 IAFIS shall maintain the Computerized Contributor File which contains contributor data (e.g., list of addresses) for Authorized Contributors.

The contributor data will be used for validation of incoming transactions and dissemination of responses.

FR437 IAFIS shall support the association of discontinued (retired) Contributor identifiers to another active Contributor records in the IAFIS CCA File.

FR438 IAFIS shall provide electronic responses to Authorized Contributors using contributor data (i.e., e-mail address) contained within IAFIS CCA File.

FR439 IAFIS shall generate hardcopy responses to Authorized Contributors using contributor data (i.e., mailing address) contained within IAFIS CCA File.

IAFIS will use the stored contributor data to verify the required destination when preparing responses to IAFIS submissions. These responses may be either electronic or hardcopy depending upon the

individual contributors needs. IAFIS will determine if the contributor can accept electronic or hardcopy responses and transmit the responses accordingly. If hardcopy responses are required, the resolution of the hardcopy will be of sufficient quality to meet ten-print fingerprint image comparison requirements.

3.7.2.10 NCIC ORI and Line File Maintenance

FR440 IAFIS shall accept NCIC ORI File Maintenance message in accordance with the III Operation and Technical Manual.

FR441 IAFIS shall update the NCIC ORI File using the data contained within the NCIC ORI File Maintenance message.

The IAFIS NCIC ORI file will be kept in sync with NCIC for message validation purposes.

FR442 IAFIS shall accept NCIC Line File Maintenance message in accordance with the III Operation and Technical Manual.

FR443 IAFIS shall update the NCIC Line File using the data contained within the NCIC Line File Maintenance message.

The IAFIS NCIC Line file will be kept in sync with NCIC for message validation purposes.

3.7.2.11 Computerized Records Sent File Maintenance

The CRS database, maintained by III, contains records of those agencies that receive copies of responses.

FR588 IAFIS shall provide the capability to store all the necessary information for agencies that receive copies of responses in the Computerized Records Sent File.

3.7.3 Repository Management

This section provides functional requirements specific to the maintenance of the IAFIS Repositories. The IAFIS will consist of the following repositories:

- Subject Criminal History File: This file will contain FBI number, and descriptive information including all identifying numbers, names (and aliases) and criminal history records for each subject.
- Criminal Ten-Print Fingerprint Image Master File: This file will contain composite fingerprint images and the associated FBI number.
- Criminal Ten-Print Fingerprint Features Master File: This file will contain fingerprint features, biographic data, and the associated FBI number.
- Civil Subject File: This file will contain Civil Record Number, and descriptive information including all identifying numbers, names (and aliases) for each subject.
- Civil Ten-Print Fingerprint Image Master File: This file will contain fingerprint images and the associated Civil Record Number. There may be more than one record for an individual.
- Civil Ten-Print Fingerprint Features Master File: This file will contain fingerprint features, biographic data, and the associated Civil Record Number.

- Ten-Print Certification File: This file will contain a copy of the original criminal or civil submission that updated an existing criminal record or criminal submissions that created new criminal records.
- Criminal Subject Photo File: This file will contain photographic images (mug shots).
- Unsolved Latent Fingerprint Image File: This file will contain the images of the unsolved latent fingerprints that meet the criteria for inclusion.
- Unsolved Latent Fingerprint Features File: This file will contain the fingerprint features of unsolved latent fingerprints and descriptive data.
- Special Latent Cognizant Ten-Print Image File(s): These files will contain images of the special latent cognizant fingerprints, which meet the criteria for inclusion.
- Special Latent Cognizant Features File(s): These files will contain fingerprint features of special latent cognizant fingerprints.
- Major Case Print File: This file will contain images of major case prints. Each set of major case prints may consist of images of multiple standard and non-standard formats. Textual data will also be stored in the file.

FR444 IAFIS shall maintain multiple IAFIS repositories to support the User Services.

FR646 IAFIS shall maintain a Shared Want Image File (SWIF) that is supported by IAFIS shared data updates.

FR647 IAFIS shall maintain a Shared Want Directory (SWD) that is supported by IAFIS shared data updates.

FR648 IAFIS shall maintain a Shared Want Activity Log (SWAL) that is supported by IAFIS shared data updates.

The SWIF, SWD and SWAL will be maintained on the SSC/FBI at the DOJ Rockville, MD facility. Features are extracted by IDENT from the images provided in the Shared Want Image File and maintained in the DHS Shared Want Directory for search by IDENT.

FR649 IAFIS shall maintain a Shared Watch Image File that is supported by IDENT shared data updates.

FR650 IAFIS shall maintain a Shared Watch Directory that is supported by IDENT shared data updates.

FR651 IAFIS shall maintain a Shared Watch Activity Log that is supported by IDENT shared data updates.

Features are extracted from the images provided in the Shared Watch Image File and maintained in the FBI Shared Watch Directory for search by IAFIS. These files will be maintained in the CJIS Data Center at the Clarksburg, WV facility.

3.7.3.1 Bulk Data Export

FR445 IAFIS shall write selected information contained in IAFIS repository(s) to media (e.g. CD, DVD, etc.) as part of a bulk media export request.

NGI-598

3.7.3.2 Repository Record Maintenance Log

FR446 IAFIS shall maintain a repository maintenance transaction log for each repository.

The repository maintenance log will contain add, deletes, modification of repository data at the record level. This repository maintenance log will assist System Administrators and Database Administrators in recovering from database failures or inadvertent actions.

FR447 IAFIS shall create an entry in the repository maintenance transaction log pertaining to record creation/deletion/update actions for each.

FR448 IAFIS shall support the use of the repository maintenance transaction log to restore the repository to a point in time in the past.

3.7.4 System Administration

The SA function is responsible for handling all system alarms, errors, system diagnostics, and system data backup and restore, system start and shutdown, resource allocation, and manual control of application/transaction processing priorities. These functions will be performed from the IAFIS Systems Management Center, the duty station of the Central System Administrators and Systems Security Administrators.

FR449 IAFIS shall allow authorized System Security Administrators to terminate any or all transactions and processes occurring in any environment independent of other IAFIS environments.

FR450 IAFIS shall allow authorized System Administrators to terminate any or all transactions and processes occurring in any environment independent of other IAFIS environments.

The System Security Administrators and System Administrators will be able to dynamically determine and reconfigure all resources available to each system environment without affecting the performance, availability, data confidentiality, and data integrity of another environment.

FR451 IAFIS shall support centralized control and display of system administration functions.

FR452 IAFIS shall support centralized control and display of system security administration functions.

FR453 IAFIS shall report system alarms to centralized system administration display.

IAFIS will report alarms for various system thresholds (e.g., file system capacity, network traffic, server utilization, etc.).

FR454 IAFIS shall support an Authorized System Administrator initiating diagnostic testing of IAFIS or identified systems/functions.

FR455 IAFIS shall support an Authorized System Administrator initiating and controlling system data backup and restore functions. NGI-599

FR456 IAFIS shall support an Authorized System Administrator initiating start command for each component IAFIS system allowing for the orderly start of IAFIS operations.

FR457 IAFIS shall support an Authorized System Administrator initiating shutdown command for each component of IAFIS system allowing for the orderly shut down of IAFIS operations.

FR458 IAFIS shall support an Authorized System Administrator reallocating of resources to level the processing workload.

FR459 IAFIS shall support an Authorized System Administrator changing transaction processing priorities.

FR460 IAFIS shall provide an Authorized System Administrator with the ability to cancel a transaction being processed, suspend a transaction, and redirect processing to another work queue.

FR652 IAFIS shall support automated scripts that daily check the availability of shared data processing servers.

FR653 IAFIS shall provide visual alarms to inform system operators or administrators of selected events or violations from the set of system parameters.

FR654 IAFIS shall support shared data terminals or workstations that provide direct access in a controlled environment.

The FBI will permit DHS system support personnel physical access to the DHS equipment contained in the SSC/DHS located at the CJISD Clarksburg, WV facility as per the CJIS Facility Security Access Policy and the Data Center Policy.

3.7.5 Manage Workflow and Work Queues

The Manage Workflow function will be responsible for managing transactions through their complete processing cycle.

FR461 IAFIS shall provide a workflow management capability.

IAFIS will support the control, sequencing, management, input and output of transactions that are processed by IAFIS as part of the workflow management function. The workflow management capability will ensure transactions are processed in the appropriate manner and completed on a timely basis.

FR462 IAFIS shall manage the processing of each transaction based on the transaction type and transaction processing rules.

FR463 IAFIS shall assign tasks to a work queue consistent with transaction processing rules.

Workgroup Loading will maximize productivity of IAFIS transaction processing. IAFIS will support rapid reassignment of work staff.

FR464 IAFIS shall allow an Authorized System Administrator the ability to adjust the rate of transactions input into IAFIS.

NGI-600

FR465 IAFIS shall collect data and statistics needed to support the management of work queues.

3.7.6 System Backup and Recovery

IAFIS backup and recovery functions will support System Administrator procedures to backup and recover system configurations, application software, and data. All IAFIS data and software necessary for recovery will be capable of being electronically backed-up on a media that can be stored off-site. Recovery operations will be capable of providing partial restoration as well as complete IAFIS operational recovery.

FR466 IAFIS shall support the creation of backup data for IAFIS repository data.

FR467 IAFIS shall support the creation of backup data for IAFIS system files.

FR468 IAFIS shall support the creation of backup data for IAFIS application files.

FR469 IAFIS shall support the recovery of IAFIS repository data from backup files.

FR470 IAFIS shall support the recovery of IAFIS system files from backup files.

FR471 IAFIS shall support the recovery of IAFIS application files from backup files.

FR472 IAFIS shall ensure that core IAFIS services are available during backup operations.

FR473 IAFIS shall support export of backup data to removable media.

The backup data produced the IAFIS system will be stored off-site, in a storage facility having a controlled and secure environment. The storage site must be sufficiently removed from the primary IAFIS site so as not to expose it to the same risks that could disable the primary site.

3.7.7 System Interfaces and Communication Management

The System Interfaces and Communications Management function will support IAFIS communications with the other systems via various networks such as CJIS, NCIC and Nlets networks. This function also identifies requirements for the management of the electronic communications internal to IAFIS.

FR474 IAFIS shall support an interface to NCIC in accordance with the III Operation and Technical Manual.

FR528 IAFIS shall support an interface to NCIC in accordance with the NCIC Operating Manual.

FR475 IAFIS shall support an interface to Nlets in accordance with the Nlets Users Guide.

FR476 IAFIS shall collect communications status information on external system interfaces.

IAFIS communication status information will include traffic flow, traffic status, line status, traffic queuing, and communication error detection between the networks and IAFIS.

FR477 IAFIS shall report communications status of external system interfaces.

FR478 IAFIS shall collect communications status information on internal system interfaces.

IAFIS communication status information will include traffic flow, traffic status, traffic queuing, and communication error detection between the networks and IAFIS.

FR479 IAFIS shall report communications status of internal system interfaces.

FR527 IAFIS shall support an interface to the CJIS WAN in accordance with the latest EFTS version.

FR529 IAFIS shall support an interface to the Special Functions System.

3.7.8 System Training and Analysis Support

This section provides all functional requirements specific to the training and analysis support for the IAFIS.

FR505 IAFIS shall provide authorized FBI System Administrators with Subject Search miss analysis tool capabilities.

FR586 IAFIS shall provide authorized FBI Service Providers with training capabilities.

FR587 IAFIS shall provide authorized FBI System Administrators with training capabilities.

3.7.9 Transaction History

The history records will be used to perform transaction audits and to generate statistical reports on IAFIS operations.

FR480 IAFIS shall collect transaction data for all transactions.

The routine transaction status data will include transaction identification, status, and processing date/time.

FR481 IAFIS shall allow Authorized FBI Service Provider access to transaction history data.

FR482 IAFIS shall allow Authorized FBI Service Provider to view transaction history data.

FR483 IAFIS shall allow Authorized FBI Service Provider to print transaction history data.

IAFIS will also provide access to the history records in order to generate statistical reports on IAFIS performance and activity.

FR484 IAFIS shall provide the capability to generate statistical reports based on transaction history data.

NGI-602

FR485 IAFIS shall retain transaction history data.

FR506 IAFIS shall record Subject Search request information to support a Subject Search Miss Analysis Tool.

3.7.10 User Fee Billing Processing

IAFIS will collect user fee history data for IAFIS chargeable fingerprint and name search transactions. IAFIS will maintain administrative user fee data (tables, files, matrices) that support the calculation of user fees and generation of user fee bills. IAFIS will generate user fee bills and reports and provide capabilities to edit (correct) user fee bills.

FR486 IAFIS shall collect user fee history data.

FR487 IAFIS shall calculate user fees for each chargeable IAFIS fingerprint identification processing and name search transaction based on user fee history data.

FR488 IAFIS shall allow Authorized FBI Service Providers access to user fee history, administrative, and billing data.

FBI Service Provider access to user fee history, administrative, and billing data will assist them in responding to user fee inquires from authorized user.

FR489 IAFIS shall provide capabilities for Authorized FBI Service Providers to maintain (i.e., add, delete, and modify) user fee administrative data.

FR490 IAFIS shall provide capabilities for Authorized FBI Services Providers to maintain user fee bills.

FR491 IAFIS shall assign a fee for each chargeable transaction.

FR492 IAFIS shall support generation of user fee bills.

FR493 IAFIS shall provide ability to generate hardcopy user fee bills.

IAFIS will provide capabilities to generate hardcopy user fee bills for the FBI Finance Division.

FR494 IAFIS shall provide ability to generate softcopy user fee bills.

IAFIS will provide capabilities to generate softcopy (electronic) user fee bills for the FBI Finance Division.

FR495 IAFIS shall support generation of user fee reports.

FR496 IAFIS shall retain user fee billing history data.

FR497 IAFIS shall retain user fee administrative data.

FR498 IAFIS shall provide the capability to regenerate user fee bills.

This Page Left Intentionally Blank.

4 OPERATIONAL REQUIREMENTS

This section describes the non-functional requirements, or general operational characteristics of the IAFIS as a whole.

4.1 Security

This section describes the IAFIS data confidentiality and data integrity requirements. IAFIS security requirements are based on the security policy, threats, and system configuration.

The provisions of the Privacy Act of 1974 and the Computer Security Act of 1987, levy certain requirements on departments and agencies of the executive branch of the Federal Government. The Privacy Act specifies that information should be protected against unauthorized access, alteration, or distribution. The Computer Security Act mandates that a System Security Plan must be prepared for all information systems in the Federal Government that store or process sensitive information. The IAFIS security requirements are based upon the CJISCAPP, the FBI MIOG Part II, Section 35, and *DOD 5200.28-STD*.

NFR1 IAFIS shall comply with all applicable federal and agency guidelines and requirements that relate to the development and operation of IAFIS.

From the security perspective, IAFIS will have two types of users: direct users, and indirect users. Direct users are those who login to an IAFIS segment with an interactive session, including operators, service providers, and specialists. Indirect users submit messages through NCIC, Nlets, or the CJIS WAN but do not have interactive sessions. Throughout this section, a reference to "users" refers to both direct and indirect users. Access to the IAFIS is controlled by rules that restrict individual users according to their system defined roles or organizational membership and need-to-know requirements. The System Security Administrator has the responsibility for ensuring that all users are assigned their proper role(s).

4.1.1 IAFIS Direct User Accessibility

NFR2 IAFIS shall provide direct user identification and authentication for controlling access to IAFIS.

4.1.1.1 IAFIS Roles and Privileges for Direct Users

NFR3 IAFIS shall provide direct users, Authorized FBI Service Providers, with access to IAFIS functions, processes and objects based upon assigned user profiles.

IAFIS will prevent a requester from executing any process or function or assuming any role not specified in the requester's profile or implicit in any roles or organizational memberships associated with the identifier. In addition, IAFIS will provide transaction accountability to each direct and indirect user.

4.1.1.2 IAFIS Login and Authentication for Direct Users

NFR4 IAFIS shall provide a unique login capability for each Authorized FBI Service Provider.

An Authorized FBI Service Providers login will include both a unique identifier and password.

NFR5 IAFIS shall authenticate the FBI Service Provider using an assigned unique identifier and password during each login attempt.

NFR6 IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

The System Security Administrator will have the capability to delegate some or all System Security Administrator role privileges to specific users who may, if so stipulated by the System Security Administrator, further delegate such privileges. Delegation of privileges will always be hierarchical, with the System Security Administrator at the top of the hierarchy.

NFR7 IAFIS shall display the date, time, workstation identifier and facility of the last login attempt for the authenticated FBI Service Provider.

NFR8 IAFIS shall not display the FBI Service Providers password when entered for authentication purposes.

NFR9 IAFIS shall require Authorized FBI Service Providers to change their password at the expiration of a time period specified by the System Security Administrator.

IAFIS will automatically notify direct users in advance that a change of their password is required. The system will generate an audit record when an authenticator has exceeded its maximum lifetime and prevent such individuals from performing a login until the System Security Administrator changes the personal authenticator. In addition, the System Security Administrator will be able to change an individual's personal authenticator without having to know the individual's current password.

NFR10 IAFIS shall not display the FBI Service Provider password when entered as part of a password change.

NFR11 IAFIS shall prohibit access to users attempting to login using an invalid or expired login ID or password.

NFR12 IAFIS shall require an FBI Service Provider password to be compliant with the CJIS CAPP.

NFR13 IAFIS shall prohibit the reuse of the last five passwords used by an individual Authorized FBI Service Provider.

NFR14 IAFIS shall store FBI Service Provider passwords in encrypted form in a protected personal authenticator file.

IAFIS will ensure that encryption will be by "one-way" encryption, i.e., the key shall be embedded in the personal authenticator.

4.1.1.3 Provide Role Based Access Control for Direct Users

NFR15 IAFIS shall enforce access control rules to ensure that system processes, functions, and data objects are accessed only by Authorized Service Providers or Authorized System Administrators, as explicitly defined by assigned role or organizational membership.

All attempts to modify, violate, or circumvent role based access control rules will generate a security audit record.

4.1.1.4 Prevent Multiple Simultaneous IAFIS Logins by Direct Users

NFR16 IAFIS shall prohibit Authorized FBI Service Providers from logging into IAFIS more than once concurrently.

As defined by the System Security Administrator, the system will prevent a direct user from logging in more than once without first properly terminating a session as defined by the System Security Administrator. All unsuccessful attempts to login will generate a security audit record.

4.1.2 Indirect User Accessibility

NFR17 IAFIS shall provide indirect user identification for controlling access to IAFIS.

4.1.2.1 Provide Secure IAFIS Access to External Systems

NFR18 IAFIS shall ensure that all arriving messages from external IAFIS systems request only those functions and data authorized to the originator of the message.

4.1.2.2 Communications Control

This section identifies requirements for IAFIS message access, traffic control, and security measures that enhance the Indirect User identification and authentication protection services provided by the CJIS, NCIC and Nlets networks.

NFR19 IAFIS shall require all remote messages from users, not authenticated directly by IAFIS, to be inspected by a message access control function.

This function will ensure that:

- Every received message has a valid ORI, and is a message type and purpose code for which the ORI has authorization,
- Every received message is uniquely identified and logged as to date and time of receipt; and
- Nothing in any message can be executable or can attempt to circumvent normal processing or gain access to privileged system functions.

NFR92 IAFIS shall require that every received message has a valid ORI, message type and purpose code for which the contributor has authorization.

NGI-607

NFR93 IAFIS shall require that every received message is uniquely identified and logged as to date and time of receipt.

NFR94 IAFIS shall prohibit any message from circumventing normal processing.

NFR95 IAFIS shall prohibit any message from gaining access to privileged system functions without authorization.

Failure of a message to include an ORI and a legitimate and authorized transaction type will cause rejection of the message and shall cause an audit record to be generated.

NFR20 IAFIS shall prohibit automatic responses required by receipt and processing of an external, automated message to IAFIS from being released and returned without first being matched against the message that requested a response.

4.1.3 Security Administration

NFR21 IAFIS shall support security administration by the System Security Administrators, each of whom will define and control direct user authentication, profiles, roles, and data access rights as well as workstation functions.

IAFIS will have numerous FBI service providers and operators. In addition, specialists from federal agencies may have direct access to IAFIS. More than one direct user may use the same IAFIS workstation in the course of a 24-hour day and the workstation may support a variety of functions. The System Security Administrator(s) will be able to execute these responsibilities from a central location.

NFR22 IAFIS shall provide the capability for a System Security Administrator deny or allow access to system resources, and monitor local transactions.

NFR23 IAFIS shall provide the capability for a System Security Administrator to disable a terminal, workstation, or access port from a central location.

NFR24 IAFIS shall support a direct user login/maintenance function for direct System Security Administrator access.

IAFIS Security Administration functionality will allow System Security Administrators to provide support to FBI Service Providers by allowing the Administrators to add, modify and delete User IDs and Passwords. In addition, Security Administrators will have the ability to limit system access to those individuals who have been both identified and authenticated.

4.1.4 System Auditing

NFR25 IAFIS shall log all system level activity (e.g. logins, functions, etc) that occurs within IAFIS in a system audit trail.

NFR26 IAFIS shall protect the IAFIS audit data from unauthorized access, modification or destruction.

The audit data will be protected by the system so that read access to it is limited to those who are authorized to access audit data. The System Security Administrator will be able to selectively audit the actions of any direct or indirect user based on the identifier.

NGI-608

The System Security Administrator will review audit data at a workstation, to determine what transactions are to be audited, to query the audit trail, to designate the time period in which audit data is to be preserved, to cause an audit trail for one or more workstations to be kept locally or at a central place, and to consolidate the various audit trails.

4.1.5 Security Auditing

NFR27 IAFIS shall log all security related activity (e.g., types of events, date and time of event, User ID, etc.) that occurs within IAFIS in a security audit trail.

For each audited event, the audit record will include auditable information (e.g., type of event, the date and time of the event, requester's identifier associated with the event, etc.). For identification/authentication events, the origin of the request (service provider and operator identifier and terminal identifier) will be included in the audit record.

NFR28 IAFIS shall provide segment level audit log data in a consolidated format.

The System Security Administrator will be able to access each segment's consolidated audit data from a single segment terminal, workstation, or console without specifying where the audit trail is physically located.

4.1.6 System and Data Integrity

4.1.6.1 System Integrity

NFR29 IAFIS shall ensure that information is protected from improper disclosure and that the services and resources composing IAFIS are impenetrable to unauthorized individuals.

A major IAFIS security goal is to ensure that the information remains as received unless changed through authorized processes and procedures.

NFR30 IAFIS shall provide hardware features for use to periodically validate the correct operation of the on-site hardware and firmware elements.

NFR31 IAFIS shall provide software features for use to periodically validate the correct operation of the on-site hardware and firmware elements.

NFR32 IAFIS shall ensure that all application software executing in the operational environment is free of any debug or system interrupt functions used to test or develop the software.

4.1.6.2 Data Integrity

NFR33 IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.

NFR34 IAFIS shall ensure that each transaction is consistent with the role(s) assigned to an individual requester.

NGI-609

IAFIS will ensure that, the mechanisms enforcing the transaction rules cannot be compromised.

4.1.7 Application Software Assurance

NFR35 IAFIS shall require that all application software satisfy the security features and access control mechanisms of IAFIS.

NFR36 IAFIS shall require that all application software satisfy the authentication guidelines of the system.

NFR37 IAFIS shall detect malicious code from entering the IAFIS environment (e.g., automated baseline tools, or virus detection tools).

NFR38 IAFIS shall prevent malicious code from entering the IAFIS environment (e.g., automated baseline tools, or virus detection tools).

4.1.8 Workstation Security

This section defines the security requirements applicable to IAFIS workstations. The purpose of these requirements is to prevent the unauthorized introduction, access, or deletion of software or data from IAFIS. Additional workstation security measures are intended to protect hardware from tampering by unauthorized personnel, and to ensure that direct access to the IAFIS is limited to authorized personnel only.

NFR39 IAFIS shall require a time-out at a terminal or workstation after a specified period of inactivity.

The inactivity time-out period of the workstations supporting shared data activities is prohibited from exceeding twenty minutes.

NFR40 IAFIS shall prohibit workstations from having any "outside" connection from the IAFIS environment without prior authorization from the System Security Administrator.

IAFIS workstations will have no dial-up capabilities without the prior authorization of the System Security Administrator.

4.1.9 IAFIS Clock Synchronization

NFR41 IAFIS shall synchronize the master IAFIS clock using an external standard reference time, such as on Coordinated Universal Time (UTC).

The processing of all IAFIS segments will be synchronized on the IAFIS master clock within a margin of 0.05 seconds.

4.1.10 Safeguard Against Object Reuse

NFR42 IAFIS shall revoke all authorizations to the information contained within an electronic media prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused storage objects.

No information, including encrypted representations of information provided by a prior subject's actions, would be available to any subject that obtains access to an object that has been released back to the system.

4.1.11 Provide Self-Protective System Architecture

NFR43 IAFIS shall provide for security-relevant software to maintain a domain for its own execution that protects itself from external interference or tampering (e.g., by modification of its code or data structures).

The resources to be protected by the security-relevant software will be isolated so that they are subject to the access control and auditing requirements.

4.2 Reliability

Reliability is the probability that a system will be able to process work correctly and completely without being aborted. Reliability is defined in terms of the system processing and fingerprint matching accuracy.

4.2.1 System Reliability

System reliability for IAFIS is the probability that the system will completely process all transactions under any condition.

NFR44 IAFIS shall process all fingerprint transactions to completion.

NFR45 IAFIS shall process all latent transactions to completion.

4.2.2 Accuracy

Accuracy is the probability that the correct identity will be selected as a candidate by the IAFIS provided that the identity exists in the repository being searched; and, that no candidate will be selected if the identity is not in the repository being searched.

NFR46 IAFIS shall have a minimum search accuracy of 95 percent, at the fingerprint search stage, in the production environment.

The determination of search accuracy will not consider fingerprint submissions that cannot be classified because of missing characteristics. The determination will not be limited to misses due to features extraction and matching. Search accuracy will take into account all other causes of missed identifications such as misreported data, data entry errors, fingerprint classification errors in both the file and search records, and less than high quality fingerprint images. Ten-Print fingerprint search accuracy will be achieved with an average number of false candidates to be compared not to exceed one (selectivity not to exceed 1).

NFR116 IAFIS shall have a minimum True Acceptance Rate (TAR) in support of data sharing that is consistent with the minimum fingerprint search reliability of 95 percent.

NFR117 IAFIS shall have a maximum False Acceptance Rate (FAR) in support of data sharing that is consistent with the IAFIS selectivity no greater than 1 on average.

NFR47 IAFIS shall identify the correct latent candidate within the top 10 positions of the candidate list at least 65 percent of the time.

NFR48 IAFIS shall identify the correct latent candidate in the top-ranked position of the candidate list at least 50 percent of the time.

NFR49 IAFIS shall perform Latent Fingerprint searches of a Latent Cognizant Features File containing 100 percent of the subjects in the Criminal Ten-Print Fingerprint Features Master File unless the search results will exceed 30 percent of the file.

IAFIS may override the 30 percent file limitation upon special approval of FBI management.

NFR50 IAFIS shall perform Latent Fingerprint searches of a Latent Cognizant Features File containing 100 percent of the subjects in the Criminal Ten-Print Fingerprint Features Master File when the search results will exceed 30 percent of the file and FBI management approves.

The 30 percent result restriction will not apply.

4.3 System Availability

System availability is the time when the application must be available for use. Required system availability is used in determining when maintenance may be performed.

IAFIS is considered to be unavailable when IAFIS is unable to satisfy the response time and workload requirements.

4.3.1 IAFIS Availability

NFR52 IAFIS shall provide functional support 24 hours a day, seven days a week.

NFR53 IAFIS shall provide 99.0% availability support to all IAFIS User Services.

NFR98 IAFIS shall be available for shared data access by IDENT a minimum of 99% measured over a one month period.

NFR54 IAFIS shall provide the capability to perform back up and maintenance activities with no impact to IAFIS availability.

NFR55 Deleted.

4.4 Supportability/Maintainability

This section includes any non functional requirement that enhances the supportability or maintainability of the system being built, including maintenance access, maintenance utilities, maintenance schedules, or architectural considerations required to provide for long term ease of maintenance.

4.4.1 Support Multiple System Environments

Because of its size, complexity, and availability requirements, IAFIS will operate in three different system environments. IAFIS must have the capability to concurrently support the system environments defined below:

- Operational: IAFIS operating in its normal configuration with complete data integrity and availability of all segments to normal users, service providers, and operators.
- Test: IAFIS providing segment and system test capabilities and operating with a separate subset of data that is unavailable to normal system users.
- Development: IAFIS providing segment development and maintenance and operating with a separate subset of data that is unavailable to normal system users.

NFR56 IAFIS shall provide the capability to concurrently support multiple system environments (i.e., operational, testing, development).

IAFIS will ensure that the performance, availability, data confidentiality, and data integrity of the operational environment is not compromised.

NFR57 IAFIS shall provide a test environment that supports the development of new hardware and software and the execution of operational tests and evaluations.

NFR58 IAFIS shall provide a development system environment that supports the development of new hardware and software and the execution of operational tests and evaluations.

The test and development environment will support assessment of IAFIS operational effectiveness and operational suitability.

4.4.2 Support IAFIS Workstations

4.4.2.1 Support Ten-Print Processing Workstations

NFR51 IAFIS shall support staff organization and 24 hours per day, seven days per week operations.

NFR59 IAFIS shall support all fingerprint service functions using an IAFIS workstation.

NFR60 IAFIS shall support fingerprint service diagnostic tools for all environments (i.e., operational, test, development).

IAFIS workstations will be capable of supporting the following Ten-print processing functionality:

- Image enhancement capabilities such as zooming, panning, contrast, and color.
- Fingerprint processing for searching against the Ten-Print data files.
- The ability to display magnified fingerprint images.
- The ability to enter different search parameters for searching the Ten-Print data files.
- The ability to review candidate lists and fingerprint images.
- The capability to classify fingerprints with the assistance of automated aids.

- The capability to display fingerprint images for comparison.
- The ability to apply compression and decompression algorithms.
- The capability to print images..

4.4.2.2 Provide Latent Processing Workstation

NFR61 IAFIS shall support all latent service functions using an IAFIS workstation.

NFR62 IAFIS shall support latent service diagnostic tools for all environments (i.e., operational, test, development).

IAFIS workstations will be capable of supporting the following latent processing functionality:

- The capability to input Latent Fingerprint submissions at no less than 500 pixels per inch (ppi) and 256 shades of gray.
- The capability to automatically and/or manually extract fingerprint features.
- The capability to classify fingerprints.
- A comprehensive digital image processing capability, such as to extract, identify, plot, and format ridge structure information.
- The ability to initiate fingerprint processing by performing Subject Searches and ad hoc inquiries.
- The ability to search against the latent cognizant files, unsolved latent image files, unsolved latent features files, and special files.
- The ability to save fingerprint features.
- The ability to review candidate lists and fingerprint images.
- The capability to display magnified fingerprint images for comparison.
- The capability to add drawings, notations, and marks to images.
- The capability to print out the search fingerprint image and the candidate fingerprint image in actual size or enlarged with and without drawings, notations, and marks.
- The capability to print images at the workstation or within the workgroup.
- Signal processing functions to reduce noise, clarify ridges, and help eliminate false fingerprint features.
- The ability to apply compression and decompression algorithms.

4.4.2.3 Provide Document Processing Workstation

NFR63 IAFIS shall support all document processing functions using an IAFIS workstation.

NFR64 IAFIS shall support document processing diagnostic tools for all environments (i.e., operational, test, development).

IAFIS workstations will be capable of supporting the following document processing functionality:

- The ability to display the document data on the workstation monitor in sufficient detail to allow easy reading of the text,
- Zooming capability on the whole document or a portion of the document,
- The ability to enhance poor images,
- The ability to apply compression and decompression algorithms,

NGI-614

- The ability to provide screen displays in data entry request format and text editing capabilities to minimize data entry errors,
- The ability to verify/validate the correctness of entered data and the presence of insufficient data and to generate appropriate notification to the service provider,
- The capability to provide access to office automation functions.

4.5 System Performance

System Performance includes non-functional requirements for response time for queries and updates, throughput, expected volume of data, and the expected volume of user activity (e.g., number of transactions during a specific time period).

4.5.1 Fingerprint Response Times

NFR65 IAFIS shall respond to a criminal fingerprint identification search within 2 hours after initiation of search on IAFIS.

NFR66 IAFIS shall respond to a civil fingerprint identification search within 24 hours after initiation of search on IAFIS.

NFR67 IAFIS shall transmit fingerprint image request responses for known subjects (i.e., subjects specified by FBI Numbers or SIDs) to authorized requesters within one hour from the IAFIS time of receipt of the request.

NFR68 IAFIS shall respond to a fingerprint image retrieval of up to 100 known subjects within 24 hours after initiation of request to IAFIS.

4.5.2 Latent Response Times

NFR69 IAFIS shall respond to a latent search within 24 hours after initiation of search on IAFIS.

4.5.3 Subject Criminal History Search Response Times

NFR70 IAFIS shall respond to a direct III Criminal Subject Search Request within 3.7 seconds after initiation of search on IAFIS.

4.5.4 Criminal Photo Storage and Retrieval Response Times

NFR71 Deleted.

NFR72 IAFIS shall respond to a criminal photo request that contains an FNU within 24 hours after the initiation of the response from IAFIS if the photo is located in the IAFIS repository.

If it is in the data file, the response time will not exceed 30.5 minutes to transmission of first data bit to the requester. IAFIS will utilize the Joint Photographic Experts Group (JPEG) compression algorithm baseline version for criminal photos. The average size of the criminal photo set will be 40KB.

NFR73 IAFIS shall perform file maintenance on criminal photos, when appropriate, within ten minutes after the initiation of the photo maintenance request.

4.5.5 Shared Data Response Times

NFR99 IAFIS shall respond to a criminal Ten-Print Fingerprint Identification Search of the IDENT shared data records within two hours after receipt by iDSM.

NFR100 IAFIS shall respond to a civil Ten-Print Fingerprint Identification Search of the IDENT shared data records within twenty four hours after receipt by iDSM.

NFR101 IAFIS shall provide a response to a shared data search within the required time allotment 95% of the time measured over a month for the end-user, not including the LESC response time.

NFR102 IAFIS shall provide the results of the shared data post processing (QA) on all positive identifications against the IDENT shared data records within 24 hours.

4.6 Workload

Workload capacity is defined as the capability of a system to handle expected data volume. For the purpose of this document, capacity requirements are stated in terms of the business and not in terms of system memory requirements or disk space.

NFR74 IAFIS shall provide the capability to meet all workload projections as described in the IAFIS System Requirements Document.

4.6.1 Support Ten-Print Processing Workload

NFR75 IAFIS shall be capable of meeting the average daily submission volume for Ten-Print processing as specified in the third row of Table 4-1A and the first row of Table 4-1B.

The anticipated total average daily volume of Ten-Print submissions by fiscal years is shown in the third row of Table 4-1A and the first row of Table 4-1B. Subject Searches and their associated Ten-Print candidate list fingerprint image comparisons will typically result in identification of less than ten percent of all civil submissions, and about two thirds of all criminal submissions. Ten-Print submissions for which Subject Search does not result in a candidate list require feature-based processing. The average daily volume of Ten-Print submissions that will require feature-based processing is shown in the fifth row of Table 4-1A and the third row of Table 4-1B.

Table 4-2 shows the size of the Ten-Print criminal subject database by fiscal year. The growth from year to year is attributable to non-identified retained criminal submissions.

NFR76 IAFIS shall be capable of meeting the average daily volumes of Ten-Print submissions requiring features-based processing as specified in the fifth row of Table 4-1A and the third row of Table 4-1B.

NGI-616

NFR77 IAFIS shall be capable of storing data in the Subject Criminal History File, the Criminal Ten-Print Fingerprint Image Master File, and the Criminal Ten-Print Fingerprint Features Master File for the number of records as specified in row 2 of Table 4-2.

NFR78 IAFIS shall be capable of storing data in the Civil Subject Index Master File and the Civil Ten-Print On-Line File for the number of records as specified in row 2 of Table 4-3.

NFR79 IAFIS shall be capable of storing data in the Civil Ten-Print Fingerprint Features File shall for the number of records as specified in row 2 of Table 4-3.

NFR103 IAFIS shall enroll IAFIS shared data at least once a day.

NFR104 IAFIS shall accept shared data enrollment requests from IDENT at least once a day.

NFR105 IAFIS shall be capable of processing 1,000 IAFIS shared data demotions per day.

NFR106 IAFIS shall be capable of processing 1,000 IAFIS shared data removals per day.

NFR107 IAFIS shall be capable of processing 2,500 IAFIS shared data enrollments per day.

NFR108 IAFIS shall be capable of extracting feature vectors from IDENT shared data at a rate of 25 per day.

NFR109 IAFIS shall be capable of supporting updates to the IDENT shared data at a rate of 200 changes per day.

NFR110 IAFIS shall support a configurable number of IAQ searches per day.

Currently, IAFIS limits the number of IAQs to LESC to 80 requests per day.

NFR111 IAFIS shall be capable of conducting up to 1,000 IAFIS Ten-Print Identification searches per day against the IDENT shared data records.

NFR112 IAFIS shall be capable of performing 1,000 manual image comparisons of IAFIS Ten-Print submissions against the IDENT shared data records per day.

NFR113 IAFIS shall have the storage capacity for 1,000,000 shared data records from IAFIS.

NFR114 IAFIS shall have the storage capacity for 13 million IAFIS shared data Activity Log entries over five years.

NFR115 IAFIS shall have the storage capacity for 1,000,000 shared data records from IDENT.

4.6.2 Support Latent Fingerprint Processing Workload

NFR80 IAFIS Latent Fingerprint processing shall be capable of meeting the average daily submission volumes as specified in the first, second and third row of Table 4-4A.

The type and volume of daily Latent Fingerprint submissions and searches of the Latent Cognizant Features file are shown in Table 4-4A. The first row of Table 4-4A identifies the daily volume of Latent Fingerprint submissions. This volume includes both electronic submissions (determined to be AFIS searchable by the submitting agency) and AFIS searchable Latent Fingerprints used to support latent physical evidence submissions. The quality of submitted Latent Fingerprints received by mail will be evaluated for AFIS processing suitability by LFPS.

The second row of Table 4-4A identifies the number of daily remote latent search requests. This row shows the number of single AFIS searchable Latent Fingerprints developed and determined to be AFIS searchable by the submitting agency.

The third row of Table 4-4A identifies the total daily volume of all latent cognizant fingerprint submission and search types. These volume totals will be shared on the basis of a 50-50 split between IAFIS requesters (50% federal requesters and 50% state and local requesters).

Each AFIS searchable Latent Fingerprint submission and search request will result in a response which is a candidate list, a poor suitability for conclusive comparison, or a notification that the 30% threshold limit has been exceeded. When a candidate list response is produced, it will be accompanied by Ten-Print fingerprint images of one or more of the top ranked candidates on that list.

NFR81 IAFIS shall be capable of meeting the average daily Latent Fingerprint submission and search volumes for Latent Fingerprint submissions as specified in the last row of Table 4-4A.

NFR82 IAFIS shall provide the capacity to store fingerprint features data in the Latent Cognizant Features file for 100% of the subjects in the Criminal Ten-Print Fingerprint Features Master file.

NFR96 IAFIS shall support a maximum Special Latent Cognizant File capacity of 1.5 million images.

NFR83 IAFIS shall provide the capacity to store fingerprint data in the Unsolved Latent Fingerprint Image File and the Unsolved Latent Fingerprint Features File for the number of subjects as specified in rows 5 and 6 of Table 4-2.

NFR84 IAFIS shall provide the capacity to store fingerprint data in the Special Latent Cognizant Image Files and Special Latent Cognizant Features Files for the total number of subjects as specified in row 7 of Table 4-2.

The system will be capable of creating up to 100 Special Latent Cognizant Image files and 100 corresponding Special Latent Cognizant Features files. The total size of all of these special latent cognizant files will not exceed the number of subjects shown in row 7 of Table 4-2.

4.6.3 Support Subject Criminal History File Processing Workload

NFR85 IAFIS shall be capable of processing the average daily volume of criminal identification requests and searches as specified in row 7 of Table 4-5, and of meeting the average daily volume of criminal history requests as specified in row 8 of Table 4-5.

Table 4-5 identifies daily volumes through the fiscal year 2012 for the following:

- Criminal Identification requests,
- NCIC (QWI) generated subject inquiry requests,
- Identification for Firearms Sales checks,
- Ten-Print submission Subject Searches,
- Document processing Subject Searches, and
- Criminal history requests.

4.6.4 Support Document Processing Workload

NFR86 IAFIS shall be capable of meeting the average daily submission volume of dispositions, expungements, and miscellaneous transactions, as specified in Table 4-6.

Table 4-6 identifies the average daily volume of document receipts per day through the fiscal year 2012 for the following:

- Dispositions
- Expungements
- Correspondence and miscellaneous documents

4.6.5 Additional IAFIS Workloads

NFR87 IAFIS shall be capable of meeting the average daily workload of submissions and requests as specified in Table 4-7.

Table 4-7 identifies the average daily number of photo submissions and requests for the fiscal years 2003 through 2012. Table 4-7 also identifies the average daily volume of Fingerprint Image Requests.

NFR88 IAFIS shall be capable of meeting the average daily workload of photo image requests and submissions as specified in Table 4-7.

NFR89 IAFIS shall be capable of meeting the average daily workload of Fingerprint Image Requests as specified in Table 4-7.

NFR90 IAFIS shall be capable of handling an average daily volume of 100 ad hoc Subject Search inquiries against the Subject Criminal History File.

NFR91 IAFIS shall be capable of handling an average daily volume of 100 ad hoc Subject Search inquiries against the 50 for Civil Subject Index Master File.

4.7 System Characteristics

NFR97 IAFIS shall adhere to the current CJIS Data Center and Facility Management policies when defining the environment in which IAFIS is located.

Table 4-1A Daily Ten-Print Submission Volume by Fiscal Year[1,2]

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Total Daily Criminal Submissions[3] (Percent Criminal)	24,953 (49%)	26,058 (50%)	28,340 (48%)	33,064 (46%)	35,460 (43%)	38,033 (41%)	40,795 (39%)	43,760 (37%)	46,943 (36%)	50,362 (34%)
Total Daily Civil Submissions[4] (Percent Civil)	25,808 (51%)	26,540 (50%)	30,308 (52%)	39,223 (54%)	46,981 (57%)	54,235 (59%)	62,553 (61%)	74,130 (63%)	84,373 (64%)	96,248 (66%)
Total Daily Submissions	50,761	52,598	58,648	72,287	82,441	92,268	103,348	117,890	131,316	146,609
Daily Volume Requiring Only Subject Search ***Criminal*** ***Civil***	22,662 17,629 5,033	21,604 18,226 3,378	23,766 19,660 4,106	28,244 23,145 5,099	30,930 24,822 6,108	33,674 26,623 7,051	36,688 28,556 8,132	40,269 30,632 9,637	43,829 32,860 10,969	47,765 35,253 12,512
Daily Volume Requiring Feature-based Processing[5] ***Criminal*** ***Civil***	28,099 7,324 20,75	30,994 7,831 23,163	34,882 8,680 26,202	102,287 63,064 39,223	112,441 65,460 46,981	122,268 68,033 54,235	103,348 40,795 62,553	117,890 43,760 74,130	131,316 46,943 84,373	146,609 50,362 96,248
Daily Non-Identification Criminal Retains	6,318	6,458	6,982	8,266	8,865	9,508	10,199	10,940	11,736	12,590
Daily Civil Retains	5,657	8,130	8,661	11,767	14,094	16,271	18,766	22,239	25,312	28,874

[1] Submission volumes measured as EFCON receipt. Criminal submissions include: AMN, CAR, CARC, CNA, CNAC, DEK, DEU, IAMN, ICAR, ICNA, IDEK, IDEU, and MPR. Civil submissions include: DOCE, EMUF, FANC, FAUF, FIDO, FNCC, FOID, FUFC, IFANC, IFAUF, IMAP, INFUF, MAP, MAPC, NFDP, NFFC, NFUE, and NFUF. AMN, DEU, and MPR are also searched against civil repository.

[2] Daily volume is obtained by dividing total volume of FY by number of days (365 or 366) in FY.

[3] Includes CARS generated from TPRS under IDENT/IAFIS V1.2. To obtain submission volumes for regular weekday multiply by 1.22. See Table 4-1 C.

[4] Includes the following initiatives: DOD, HSPD-12, HAZMAT, and PROTECT ACT. To obtain submission volumes for regular weekday multiply by 1.36. See Table 4-1C.

[5] Includes III Verify Idents from FY 2006. CMF Consolidation Project of 30,000 feature searches per day for FY 2006, 2007, 2008.

TABLE2 Table 4-1B Daily Remote Ten-Print Submission Volume by Fiscal Year (TPIS, TPFS, TPRS)

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Total Daily Submissions[6]	1,029	2,126	4,415	20,000	22,000	24,200	26,620	29,282	32,210	35,431
Daily Volume Requiring Feature-based Processing	1,029	2,126	4,415	20,000	22,000	24,200	26,620	29,282	32,210	35,431

Table 4-1C Average Weekday Ten-Print Submission Volume by Fiscal Year[7]

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Total Daily Criminal Submissions	30,443	31,790	34,575	40,338	43,261	46,400	49,769	53,387	57,271	61,441
	(46%)	(47%)	(46%)	(43%)	(40%)	(39%)	(37%)	(35%)	(33%)	(32%)
Total Daily Civil Submissions	35,099	36,095	41,218	53,344	63,894	73,760	85,073	100,817	114,747	130,897
	(54%)	(53%)	(54%)	(57%)	(60%)	(61%)	(63%)	(65%)	(67%)	(68%)
Total Daily Submissions	65,541	67,885	75,793	93,681	107,155	120,160	134,842	154,203	172,018	192,338

[6] FY 2006 set at 20,000 reflecting IDENT/IAFIS V1.2 workload for TPRS. 10% growth rate thereafter.

[7] Based on Table 4-1A.

Table 4-2 Criminal Ten-Print and Latent Files' Size By Fiscal Year

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Number of Ten-Print Subjects at Start of Year	41,588,597	43,626,920	45,730,625	47,972,901	50,639,975	53,500,374	56,576,699	59,867,396	63,397,265	67,183,933
Number of Ten-Print Subjects at End of Year	43,626,920	45,730,625	47,972,901	50,639,975	53,500,374	56,576,699	59,867,396	63,397,265	67,183,933	71,257,475
Growth as Percent of File Size	4.9%	4.8%	4.9%	5.6%	5.6%	5.8%	5.8%	5.9%	6.0%	6.1%
Number of Latent Cognizant Subjects	43,626,920	45,730,625	47,972,901	50,639,975	53,500,374	56,576,699	59,867,396	63,397,265	67,183,933	71,257,475
Number of Unsolved Latent Subjects (LFPS and Federal)[8,9]	8,845	12,282	15,795	18,795	21,795	24,795	27,795	30,795	33,795	36,795
Number of Unsolved Latent Subjects (State and Local)[8,10]	19,610	34,967	63,389	93,389	123,389	153,389	183,389	213,389	243,389	273,389
Number of Special Latent Cognizant Subjects[11]	69,405	77,702	79,386	144,386	174,386	204,386	234,386	264,386	294,386	324,386

[8] IAFIS can support a maximum total of 250,000 divided equally between the two.

[9] FY 2006 number obtained by prorating actual numbers up to end of April, 2006 which is a one year increase of about 3,000. This is used as annual increase for FY 2007-2012 as well.

[10] FY 2006 number obtained by prorating actual numbers up to end of April, 2006 which is a one year increase of about 30,000. This number is used as annual increase for FY 2007-2012 as well. It reaches the maximum allocation of 125,000 by end of FY 2007.

[11] IAFIS can support a maximum of 1,500,000. It includes terrorists, deceased unknown as well as Interpol subjects. FY 2006 number obtained by prorating actual numbers to end of April, 2006 which is a one year increase of about 65,000. An annual increase of 30,000 is used for FY 2007-2012.

Table 4-3 Civil Ten-Print Subject Database Size By Fiscal Year

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Number of Subjects at Start of Year	1,828,752	3,893,540	6,861,044	10,022,265	14,317,224	19,461,621	25,416,624	32,266,227	40,383,454	49,622,309
Number of Subjects at End of Year	3,893,540	6,861,044	10,022,265	14,317,224	19,461,621	25,416,624	32,266,227	40,383,454	49,622,309	60,190,286
Annual Growth in the Number of Subjects in	112.9%	76.2%	46.1%	42.9%	35.9%	30.6%	26.9%	25.2%	22.9%	21.3%

Table 4-4A Daily Latent Fingerprint Submissions and Searches-Latent Cognizant File (Fiscal Year)

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Latent Print Submissions[12]	11	33	958	50	55	61	67	73	81	89
Remote Latent Search Requests[13]	97	173	225	293	380	494	643	835	1,086	1,412
Total Latent Submissions and Remote Searches	108	206	1,183	343	435	555	709	909	1,167	1,500
Searches of Special Latent Cognizant Files[14]	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000

Table 4-4B Daily Miscellaneous Latent Workloads (Fiscal Year)

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Penetration Query[15]	6	11	9	11	13	16	19	22	27	32
Repository Statistics Query	0	0	0	10	10	10	10	10	10	10
Search Status and Modification Query[15]	12	17	13	16	19	22	27	32	39	47

[12] The spike in FY 2005 reflects a special project. 10% annual growth rate from FY 2007. Within agreed upon daily allocation of 218.

[13] Annual growth rate of 30% from FY 2006. Exceeds daily allocation of 834 in FY 2010, 2011, and 2012.

[14] Workload represents peak daily demand for a short duration due to natural disasters (e.g., Katrina disaster), terrorist acts, etc.

[15] Assumes annual growth rate of 20% from FY 2006.

Table 4-5 Daily Criminal Subject Identification Requests, Subject Searches, and Criminal History Requests by Fiscal Year

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Criminal Subject Identification Requests[16]	347,061	407,916	488,412	580,563	690,591	822,017	979,059	1,166,772	1,391,219	1,659,664
NCIC (QWI) Generated Subject Inquiry Requests[17]	1,362	1,636	2,333	2,800	3,360	4,032	4,838	5,806	6,967	8,360
NICS[18]	23,310	23,565	24,392	26,202	26,595	26,994	27,399	27,810	28,227	28,650
Subtotal Criminal Subject Identification Requests	371,733	433,117	515,137	609,565	720,546	853,042	1,011,295	1,200,388	1,426,412	1,696,674
Subject Searches from Ten-Print Submissions[19]	45,950	47,500	53,157	65,420	74,609	83,502	93,530	106,690	118,841	132,681
Subject Searches from Document Processing	18,062	12,961	7,806	19,622	21,094	22,676	24,377	26,205	28,170	30,283
Total Subject Inquiries, Identification Requests, and Searches	435,746	493,578	576,100	694,607	816,249	959,221	1,129,202	1,333,283	1,573,424	1,859,639
Total Daily Criminal History Requests[20]	47,603	51,505	55,311	60,842	66,926	73,618	80,980	89,078	97,986	107,785

[16] Count of QH & QR. From FY 2006 assume annual growth rate of 20% for QH and 10% for QR.

[17] Count of QWI. Annual growth rate of 20% from FY 2006.

[18] NICS firearms & explosives background checks. FY 2006 workload based on proration of actual receipt to April 2006. 1.5% annual growth rather thereafter.

[19] Consistent with total daily ten-print submissions from Table 4-1A excluding AMN, DEU, IAMN, and IDEU as well as ten-print submissions with quoted FNUs.

[20] Count of QR. 10% annual growth rate from FY 2006 on.

NGI-625

Table 4-6 Daily Document Receipt Workloads (Fiscal Year)

	2004	2005	2006	2007	2008	2009	2010	2011	2012
Total Dispositions[21,22]	15,506	10,855	5,730	17,390	18,695	20,097	21,604	23,224	24,966
Total Expungements[23]	1,764	1,522	1,633	1,755	1,887	2,028	2,180	2,344	2,519
Total Correspondence and Miscellaneous Documents[23]	792	584	444	477	513	551	593	637	685
Total Subject Searches from Document Processing	18,062	12,961	7,806	19,622	21,094	22,676	24,377	26,205	28,170

[21] Counts include both paper and MRD dispositions.

[22] 2006 counts based on prorating of actual count to early May, 2006 and assumes 7.5% annual growth rate thereafter.

[23] 7.5% annual growth rate after FY 2005.

NGI-626

Table 4-7 Daily Photo and Fingerprint Image Requests and Submissions (Fiscal Year)

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Daily Photo Retrieve Request[24]	0	0	0	50	60	72	86	104	124	149
Daily Photo Addition[25]	1,047	1,444	2,448	3,060	3,825	4,782	5,977	7,471	9,339	11,674
Daily Photo Delete Requests[26]	0	0	0	5	6	7	9	10	12	15
	2003	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**
Daily Fingerprint Retrieve Request[27]	565	3,313	1,536	3,383	4,060	4,872	5,846	7,015	8,418	10,102
Daily Fingerprint Addition	6,318	6,458	6,982	8,266	8,865	9,508	10,199	10,940	11,736	12,590
Daily Fingerprint Delete Requests	734	710	839	959	1,028	1,103	1,183	1,269	1,361	1,460
Daily Fingerprint Image Replacement[28]	88	148	30	100	110	121	133	146	161	177

[24] Based on CPR counts; 20% annual growth rate from FY 2007.

[25] 25% annual growth rate from FY 2006.

[26] Based on CPD counts; 20% annual growth rate from FY 2007.

[27] Counts of IRQ. FY 2006 daily workload based on average of actual count till April 30, 2006. Annual growth rate of 20% from FY 2007.

[28] Counts of FIS and IFIS.

This Page Left Intentionally Blank.

BIBLIOGRAPHY

1. American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, ANSI/NIST-ITL 1-2000, NIST Special Publication 500-245, September 2000.

2. American National Standards Institute (1988), *American National Standard for Forensic Identification - Automated Fingerprint Identification Systems - Glossary of Terms and Acronyms*, ANSI/IAI 2-1988, New York, NY.

3. Assistant Secretary of Defense (1985), *Department of Defense Trusted Computer System Evaluation Criteria*, (TCSEC), DOD 5200.28 STD, Washington, DC.

4. Criminal Justice Information Services Controlled Access Protection Profile (CJISCAPP), Department of Justice, Federal Bureau of Investigation, December 8, 2003.

5. Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification (EFTS), IAFIS-DOC-01078-7.1, V7.1, May 2, 2005.

6. Department of Defense Computer Security Center (1985), *Department of Defense Password Management*, CSC-STD-002-95, Fort George Meade, MD.

7. Department of Justice Order 2640.2B, *Automated Information Systems Security*, November 16, 1988.

8. Department of Justice Order 2640.3, *Unique Identification and Authentication of Users of Automated Information Systems*, March 30, 1990.

9. Department of Justice (1991), *Code of Federal Regulations Title 28, Part 19*, National Archives and Records Administration, Washington, DC.

10. Federal Bureau of Investigation (2004), *Disposition Submission Via Machine Readable Data*, IAFIS-III-DOC-01008-2.0, February 25, 2004.

11. Federal Bureau of Investigation (2004), *Expungement Submission Via Machine Readable Data*, IAFIS-III-DOC-01007-1.1, October 20, 2003.

12. Federal Bureau of Investigation (FBI), Information Technology Life Cycle Management Directive (IT LCMD) 2.0, November 19, 2004.

13. Federal Bureau of Investigation (2006), *Machine Readable Data (MRD) Name Search Specifications*, IAFIS-DOC-01049-1.2, April 11, 2006

14. Federal Bureau of Investigation (1979), *The Identification Division of the FBI*, Washington, DC.

NGI-629

15. Federal Bureau of Investigation (FBI), *NCIC 2000 Operating Manual*, December 1999.

16. Federal Bureau of Investigation (1984), *The Science of Fingerprints: Classification and Uses*, Washington, DC.

17. Federal Bureau of Investigation (FBI) Manual of Investigative Operations and Guidelines (MIOG), Part II, Section 35 (FBI ADPT Security Manual), July 26, 1995.

18. National Bureau of Standards (1985), NBS Special Publication 500-120, *Security of Personal Computer Systems: A Management Guide*, Washington, DC.

19. National Computer Security Center (1987), *Trusted Network Interpretation*, NCSC-TG-005, Version 1, Fort George Meade, MD.

20. National Technical Information Service (1975), FIPS PUB 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Washington, DC.

21. National Telecommunications and Information Systems Security Committee, National Telecommunications and Information Systems Security Policy, NTISSP No. 200, (1987), *National Policy on Controlled Access Protection*, Washington, DC.

22. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources,* February 20, 1996.

23. Office of Management and Budget (OMB), Bulletin No. 88-16, *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information*, Washington, DC., 1988.

24. Office of Management and Budget (1985), Circular No. A-130, Management of Federal Information Resources, Washington, DC.

25. Target Enterprise Architecture, EAPO-DOC-1077-1.1, August 2005.

26. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 65), Guideline for Automatic Data Processing (ADP) Risk Analysis, August 1, 1979.

27. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 73), Guidelines for the Security of Computer Applications, June 30, 1980.

28. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 87), Guidelines for ADP Contingency Planning, March 27, 1981.

29. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 31), Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974.

30. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 112), Password Usage, May 30, 1985.

31. 5 U.S. Code 552a, Privacy Act of 1974, (Public Law 93-579), December 1974.

32. 40 U.S. Code 759, Computer Security Act of 1987, (Public Law 100-235), January 8, 1988.

ACRONYMS

See the *IAFIS Acronym List and Glossary.*

This Page Left Intentionally Blank.

TERMS

See the *IAFIS Acronym List & Glossary*.